

All-Russian Conference

«THE RADIO-ELECTRONIC DEVICES AND
SYSTEMS FOR THE INFOCOMMUNICATION
TECHNOLOGIES» (REDS-2026)



REDS-2026



Moscow - 2026

Всероссийская конференция

“Радиоэлектронные устройства
и системы для
инфокоммуникационных
технологий”

РЭУС-ИТ 2026



ДОКЛАДЫ

Серия:
НАУЧНЫЕ КОНФЕРЕНЦИИ,
ПОСВЯЩЕННЫЕ ДНЮ РАДИО
(выпуск LXXXI)

Российского
научно-технического общества
радиотехники, электроники и связи
имени А.С. Попова

Москва - 2026

Всероссийская конференция

**«РАДИОЭЛЕКТРОННЫЕ УСТРОЙСТВА И СИСТЕМЫ ДЛЯ
ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ» (РЭУС-ИТ 2026).
ПОСВЯЩЁННАЯ «ДНЮ РАДИО».**

Россия, Москва

Даты проведения: 20 - 21 мая 2026 года.

All-Russian Conference

**"THE RADIO-ELECTRONIC DEVICES AND SYSTEMS FOR THE
INFOCOMMUNICATION TECHNOLOGIES" ("REDS-2026").**

Russia Moscow

Dates: May 20 - 21, 2026.

ДОКЛАДЫ

PROCEEDINGS



МИНИСТЕРСТВО
НАУКИ И ВЫСШЕГО
ОБРАЗОВАНИЯ
РОССИЙСКОЙ
ФЕДЕРАЦИИ



МОСКВА 2026 г.

Всероссийская конференция «Радиоэлектронные устройства и системы для инфокоммуникационных технологий - РЭУС-ИТ 2026», Москва, Россия, доклады.

Рецензенты:

проф. Аджемов А.С., проф. Бартенев В.Г., проф. Витязев В.В., проф. Дроздов Б.В., проф. Калошин В.А., проф. Постников И.И., проф. Поборчая Н.Е., проф. Потапов В.Т., проф. Степанов С.Н., проф. Хорев А.А., проф. Цимбал В.А., проф. Чиров Д.С.,

Выходные данные издания:

- УДК [004+621.396] (082)
- ББК 32.973+32.84
- В85

ISBN 978-5-905278-66-2

2



9 785905 278662

© Авторы докладов
© РНТОРЭС имени А.С. Попова



ОРГАНИЗАТОРЫ:

- | | |
|---|--|
| • Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова; | • Институт радиотехники и электроники имени В.А. Котельникова РАН; |
| • Отделение нано и информационных технологий РАН; | • Московский технический университет связи и информатики; |

ПРИ УЧАСТИИ:

- | | |
|--|--|
| • Министерство высшего образования и науки РФ; | • Московский государственный технический университет имени Н.Э. Баумана; |
| • ОАО «Концерн радиостроения «Вега»; | • Нижегородский госуниверситет им. Н.И. Лобачевского; |
| • ФГУП «НИИР»; | • Нижегородский технический госуниверситет имени Р.Е. Алексеева; |
| • Балтийский федеральный университет имени И. Канта; | • Пензенский государственный университет |
| • Владимирский государственный университет; | • Рязанский государственный радиотехнический университет; |
| • Московский авиационный институт; | • Санкт-Петербургский государственный электротехнический университет – («ЛЭТИ»); |
| • Московский энергетический институт; | • Санкт-Петербургский государственный университет телекоммуникаций; |
| • Московский институт электронной техники; | • Ульяновский государственный технический университет; |
| • Московский физико-технический институт; | • Ярославский государственный университет. |

ВСЕРОССИЙСКИЙ ПРОГРАММНЫЙ КОМИТЕТ:

Председатель:

академик РАН Панченко Владислав Яковлевич

Заместитель председателя:

академик РАН Шерemet Игорь Анатольевич

Члены Программного комитета:

проф. Аджемов А.С., д.т.н. Борисов В.П., д.т.н. Бутенко В.В.,
член-корр. РАН Верба В.С., проф. Витязев В.В.,
член-корр. РАН Дворкович А.В., проф. Петровский А.А. (Беларусь),
проф. Ямпурин Н.П.

ВСЕРОССИЙСКИЙ ОРГАНИЗАЦИОННЫЙ КОМИТЕТ:

4

Председатель:

академик РАН Никитов Сергей Аполлонович

Заместитель председателя:

академик РАН Чаплыгин Юрий Александрович

Члены Оргкомитета:

проф. Бартенев В.Г., проф. Дроздов Б.В., проф. Калошин В.А.,
проф. Поборчая Н.Е., проф. Постников И.И., проф. Приоров А.Л.,
доц. Самсонов Г.А., проф. Сергеев В.А., проф. Степанов С.Н.,
проф. Хорев А.А., проф. Чиров Д.С., проф. Шорин О.А.

Организация работы в форме пленарных и проблемно-тематических заседаний. Пленарные доклады представлены по основным направлениям работы Конференции (г. Москва, Конгресс-центр МТУСИ).

Рабочий язык конференции - *русский (английский)*.

СОДЕРЖАНИЕ:

<u>ПЛЕНАРНЫЕ ДОКЛАДЫ</u>	6
<u>СЕКЦИЯ № 2. РАДИОТЕХНИКА, РАДИОЛОКАЦИЯ, В Т.Ч. ЗОНДИРОВАНИЕ ЗЕМЛИ, РАДИОНАВИГАЦИЯ.</u>	9
<u>СЕКЦИЯ № 3. СИСТЕМЫ, СЕТИ И УСТРОЙСТВА ТЕЛЕКОММУНИКАЦИЙ, В Т.Ч. КОСМИЧЕСКИЕ, ЛАЗЕРНЫЕ, АКУСТИЧЕСКИЕ, ВОЛОКОННО-ОПТИЧЕСКИЕ И ИНЫЕ.</u>	47
<u>СЕКЦИЯ № 4. ИНФОРМАЦИОННЫЕ И ИНТЕРНЕТ-ТЕХНОЛОГИИ, В Т.Ч. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ</u>	111
<u>СЕКЦИЯ № 5. РАДИОСВЯЗЬ</u>	193
<u>СЕКЦИЯ № 6. ЗАЩИТА ИНФОРМАЦИИ, В Т.Ч. КОДИРОВАНИЕ, И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.</u>	228
<u>АВТОРСКИЙ УКАЗАТЕЛЬ.</u>	436

АДАПТИВНЫЕ АНТЕННЫЕ РЕШЕТКИ С НЕЧЕТНОЙ СИММЕТРИЕЙ

д.т.н., проф. Джиган В.И.

Национальный исследовательский университет «МИЭТ»

. В работе рассматриваются основные свойства антенных решёток (АР) как разновидности направленных антенн, которые могут формировать провалы в диаграмме направленности в направлениях на источники помех с целью подавления их сигналов в выходном сигнале решётки. Это свойство способствовало появлению адаптивных АР (ААР), которые формируют такие провалы в реальном масштабе времени, не требуя при этом никакой априорной информации об угловых положениях источников помех и их характеристиках. Так как принимаемые ААР сигналы характеризуются амплитудами и фазами, то вычисление выходного сигнала ААР и её весовых коэффициентов (ВК) выполняется в арифметике комплексных чисел. Это является источником повышенной вычислительной сложности таких алгоритмов. Однако, если ААР является нечетно-симметричной (сигналы в парах её антенн, симметричных относительно фазового центра АР, и ВК соответствующих каналов являются комплексно-сопряжёнными по отношению к друг-другу), то вычисление ВК можно производить в арифметике действительных чисел, что уменьшает в два раза сложность этого вычисления по сравнению с ААР в арифметике комплексных чисел. Кроме того, переходные процессы в ААР с нечетной симметрией в два раза короче, а подавление помех в среднем на 3 дБ больше, чем несимметричных ААР. Эти результаты подтверждены примерами моделирования трех разновидностей ААР для наземных приемников глобальных систем спутниковой навигации.

Антенная решётка (АР) – это разновидность направленных антенн [1]. В отличие от других видов таких антенн, например, зеркальных или линзовых, управление лучом (основным лепестком диаграммы направленности, ДН) в АР осуществляется не механическим, а электрическим способом, т.е. при неподвижной АР. Это является одним из преимуществ АР перед антеннами с механическим управлением лучом. Сегодня АР уже широко используются в качестве направленных антенн радиосистем различного назначения: радиолокационных, радионавигационных и радиоуправления.

Приоритет в изобретении АР принадлежит Сергею Александровичу Щелкунову (США) [2], о чем свидетельствует патент [3]. Принцип работы АР базируется на когерентном сложении радиоволн сигналов, принимаемых антеннами решётки от их источника, расположенного в дальней зоне в случае приемной АР, или на когерентном сложении сигналов в дальней зоне в случае передающей АР. Такое сложение обеспечивается в приёмных или передающих АР за счет сдвига по фазе сигналов с помощью фазовращателей.

Фазовращатели – это простейшие комплексные весовые коэффициенты (ВК) с модулем, равным единице. Однако сигналы в каналах АР можно изменять не только по фазе, но и по амплитуде. Для этого используются соответствующие комплексные ВК. Такие ВК представляют собой либо каскадно-соединенные фазовращатели и аттенюаторы, либо аттенюаторы в квадратурных каналах в аналоговых АР [1], или просто комплексные числа в цифровых АР [4].

Комплексное взвешивание сигналов АР позволяет не только изменять угловое положение её луча, но и управлять всей формой ДН. Такое управление в приемной АР можно осуществлять, например, с целью формирования в ДН провалов в направлениях на источники помех. На этом принципе основана работа адаптивных АР (ААР) [5].

Согласно [6], приоритет в области изобретения ААР принадлежит Полу Хауэллсу (Paul W. Howells, США) [7]. Адаптивные алгоритмы обрабатывают сигналы в информационной полосе частот, т.е. на нулевой промежуточной частоте, поэтому ААР должна быть цифровой [4]. Построение цифровых АР базируется на принципах программно-определяемого цифрового радио [8].

Так как сигналы, принимаемые антеннами АР, характеризуются амплитудами и фазами, то вычисление ВК ААР и её выходного сигнала реализуются в арифметике комплексных чисел. Вычисления ВК ААР базируются на классических алгоритмах адаптивной фильтрации [9]. При обработке комплексных сигналов, их вычислительная сложность (число арифметических операций, приходящихся на одну итерацию алгоритма), в четыре раза больше вычислительной сложности этих же алгоритмов, используемых для обработки действительных сигналов и реализуемых в арифметике действительных чисел.

Задача уменьшения вычислительной сложности алгоритмов работы ААР представляется актуальной. В настоящей статье рассматриваются методы, позволяющие уменьшить эту сложность и одновременно увеличить эффективность ААР в терминах длительности переходного процесса и глубины провалов в ДН направлениях на источники помех в установившемся режиме.

Достичь указанной эффективности можно, если ААР обладает нечетной симметрией. Нечетно-симметричной называется ААР, в которой отсчеты сигналов и ВК в парах каналов, чьи антенны расположены симметрично относительно фазового центра ААР, являются комплексно-сопряженными по отношению к друг-другу. В [10–12] было показано, что корреляционная матрица сигналов такой ААР является персимметричной. Её элементы симметричны не только относительно главной диагонали (как и в несимметричной ААР), но и относительно побочной диагонали.

Такая форма корреляционной матрицы позволяет реализовать алгоритм вычисления ВК нечётно-симметричной ААР в арифметике действительных чисел и при этом уменьшить вычислительную сложность данного алгоритма примерно в 2 раза по сравнению с аналогичным алгоритмом в арифметике комплексных чисел несимметричной ААР. Кроме того, в нечетно-симметричной ААР длительность переходного процесса применено в два раз меньше и подавление помех в установившемся состоянии в среднем на примерно на 3 дБ больше, чем в несимметричной ААР. Уменьшение длительности переходного процесса обусловлено оценкой корреляционной матрицы дважды на каждой итерации адаптивного алгоритма (отсчёте обрабатываемых сигналов). Оценка корреляционной матрицы входных сигналов нечётно-симметричной ААР также является более точной по сравнению с оценкой аналогичной матрицы несимметричной ААР, что обеспечивает лучшее подавление помех с помощью первой ААР по сравнению со второй ААР.

Некоторые исследования нечётно-симметричных ААР представлены в [13–21] и в ряде других работ. В частности, в [17] показано, что в наиболее общем случае нечётно-симметричной ААР, а именно в линейно-ограниченной ААР с требуемым сигналом, вычисление ВК также можно выполнять в арифметике действительных чисел и обеспечивать отмеченные выше характеристики.

Данные свойства нечётно-симметричных ААР подтверждены результатами моделирования трех разновидностей ААР для наземных приёмников сигналов глобальных систем спутниковой навигации (ГНСС). Это компенсатор помех [19], линейно-ограниченная ААР [20] и ААР предварительной обработкой входных сигналов с помощью корреляторов или согласованных фильтров [21].

Рассматриваемые ААР могут быть использованы не только в радиоприёмниках сигналов ГНСС, но и в других радиосистемах, где требования к вычислительным ресурсам, выделяемым на реализацию ААР, длительность переходного процесса и степень подавления помех являются важными характеристиками.

Литература

1. Maillou R.J. Phased array antenna handbook, 3rd ed. Artech House, Inc., 2017. – 506 p.
2. Schelkunoff S.A. A mathematical theory of linear arrays // The Bell System Technical Journal. – 1943. – Vol. 22. – № 1. – P. 80–107.
3. Schelkunoff S.A. Directive antenna system // US Patent 2286839. – 1942. – 15 p.
4. Григорьев Л.Н. Цифровое формирование диаграммы направленности в фазированных антенных решётках. – М.: Радиотехника, 2010. – 144 с.
5. Monzingo R.A., Haupt R.L., Miller T.W. Introduction to adaptive arrays, 2nd ed. SciTech Publishing, 2011. – 510 p.
6. Reed I.S. Brief history of adaptive arrays // IEEE Military Communications Conference. – Boston, MA, USA, 1985. – P. 515–518.
7. Howells P.W. Intermediate frequency side-lobe canceller // US Pattern 3202990. – 1959. – 8 p.
8. Dillinger M., Madani K., Alonistioti N. Software defined radio: architectures, systems and functions. Wiley, 2003. – 454 p.
9. Джиган В.И. Адаптивная фильтрация сигналов: теория и алгоритмы. – М: Техносфера, 2013. – 528 с.
10. Cantoni A., Butler P. Properties of eigenvectors of persymmetric matrices with applications to communication theory // IEEE Trans. Commun. – 1976. – Vol. 24. – № 8. – P. 804–809.

-
11. Nitzberg R. Application of maximum likelihood estimation of persymmetric covariance matrices to adaptive processing // IEEE Trans. Aerospace and Electronic Systems. – 1980. – Vol. 16. – № 1. – P. 124–127.
 12. Huarng K.C., Yen C.C. A unitary transformation method for angle of arrival estimation // IEEE Trans. Acoustic, Speech and Signal Processing. – 1991. – Vol. 39. – № 4. – P. 975–977.
 13. Зарицкий В.И., Кокин В.Н., Леховицкий Д.И., Саламатин В.В. Рекуррентные алгоритмы адаптивной обработки при центральной симметрии пространственно-временных каналов приема // Изв. вузов. Радиофизика. – 1985. – Том 28. – № 7. – С. 863–871.
 14. Huarng K.-C., Yeh C.-C. Adaptive beamforming with conjugate symmetric weights // IEEE Trans. Antennas and Propagation. – 1991. – Vol. 39. – № 7. – P. 926–932.
 15. Джиган В.И. Функциональная и вычислительная эффективность RLS-алгоритмов в арифметике действительных чисел для многолучевых адаптивных антенных решеток // Известия ЮФУ. Технические науки. – 2013. – № 2. – С. 29–35.
 16. Джиган В.И. Алгоритмы адаптивной линейно-ограниченной слепой обработки сигналов в цифровых антенных решетках с нечетной симметрией // Цифровая обработка сигналов. – 2015 – № 2. – С. 3–13.
 17. Джиган В.И. Нечетная симметрия вектора весовых коэффициентов симметричных антенных решеток с линейными ограничениями // Известия высших учебных заведений. Радиоэлектроника. – 2018. – № 6. – С. 323–335.
 18. Джиган В.И. Антенная решетка с частичной адаптацией на основе рекурсивных алгоритмов по критерию наименьших квадратов в арифметике действительных чисел // Радиотехника. – 2023. – № 1. – С. 144–157.
 19. Джиган В.И. Компенсатор помех в арифметике действительных чисел // Труды 32-й Международной конференции «Радиолокация, навигация, связь (RLNC-2026)» (Воронежский государственный университет, 14 – 16 апреля 2026 г.). – Воронеж, 2026. – Том 1. – С. 113–122.
 20. Джиган В.И. Линейно-ограниченная адаптивная антенная решетка в арифметике действительных чисел для радиоприемников наземной аппаратуры потребителя глобальных навигационных спутниковых систем // T-Comm: Телекоммуникации и транспорт. – 2026. – № 3. – С. 4–14.
 21. Djigan V.I. Self-steering reduced-complexity adaptive antenna array for Global Navigation Satellite Systems // Proceedings of the 27-th International Conference on Digital Signal Processing and its Applications (DSPA-2026). – Moscow, Russia, March 25 –27, 2026. – 4 p.

ODD-SYMMETRIC ADAPTIVE ANTENNA ARRAYS

Dr.Sc., Prof., Djigan V.I.

National Research University of Electronic Technology

. This paper examines basic properties of Antenna Arrays (AAs) as a type of directional antennas capable of creating notches in the radiation pattern towards interference sources, suppressing their signals at the array's output. This has led to the development of the Adaptive Antenna Arrays (AAAs), which create such notches in real time without requiring any a priori information about the angular positions of the interference sources and their characteristics. Since the signals received by the AAAs are characterized by their amplitudes and phases, the AAA output signal and its weights are calculated using complex-valued arithmetic. This is the source of the increased computational complexity of such algorithms. However, if the AAA is odd-symmetric (the signals in pairs of its antennas, symmetrical relatively the phase center of the AAA, and the weights of the corresponding channels are complex conjugates of each other), then the weights calculation can be performed using real-valued arithmetic, which halves the complexity of this calculation compared to the AAA in complex-valued arithmetic. Furthermore, the transient response in an AAA with odd symmetry is half as fast, and interference suppression is, on average, 3 dB greater than that of the asymmetric AAAs. These results are verified by the simulation examples of three types of AAAs for the ground-based receivers of the Global Navigation Satellite Systems.



СЕКЦИЯ № 2. РАДИОТЕХНИКА, РАДИОЛОКАЦИЯ, В Т.Ч. ЗОНДИРОВАНИЕ ЗЕМЛИ, РАДИОНАВИГАЦИЯ.

МОДИФИЦИРОВАННАЯ ИМИТАЦИОННАЯ МОДЕЛЬ ДОБСОНА ДЛЯ ДИСТАНЦИОННОГО ОПРЕДЕЛЕНИЯ ВЛАЖНОСТИ ПОЧВЫ

проф., д.т.н. Линец Г.И., к.т.н. Мельников С.В., асп. Гончаров В.Д.

Северо-Кавказский федеральный университет

В работе представлена модифицированная модель Добсона для дистанционного определения объёмной влажности почвы, в которой параметры свободной воды заменены характеристиками связанной воды. Выведены аналитические формулы, исключающие итерационные вычисления и позволяющие оценивать влажность по комплексной диэлектрической проницаемости. Для оценки точности и адекватности модели проведена ее валидация на основе сопоставления значений объёмной влажности, полученных в результате моделирования (с использованием модифицированной модели, а также классических моделей Добсона и Топпа), с результатами измерений влажности влагомером TDR-150 (Spectrum Technologies, щуп 20 см). Предлагаемая модель демонстрирует наилучшую точность определения влажности почвы во всем диапазоне исследований.

Влажность почвы является одним из ключевых параметров, определяющих энергетический и водный баланс земной поверхности. Количественная оценка содержания влаги в почвенном слое имеет критическое значение для широкого спектра прикладных и фундаментальных задач: от гидрологии и климатологии (прогнозирование засух, наводнений) до точного земледелия (оптимизация орошения) и мониторинга состояния экосистем [1]. В связи с этим развитие методов дистанционного зондирования Земли (ДЗЗ), позволяющих осуществлять оперативный и масштабный контроль влажности, является одним из приоритетных направлений современной геофизики и радиофизики.

Фундаментальной основой для извлечения информации о влажности почвы из данных ДЗЗ, в особенности радиолокационных и радиометрических, является комплексная диэлектрическая проницаемость (КДП). КДП выступает в роли связующего звена между непосредственно измеряемыми радиолокационными параметрами почвы (коэффициентом отражения, яркостной температурой, обратным рассеянием) и искомым физическим параметром – объёмной влажностью почвы. Высокая контрастность диэлектрической проницаемости, обусловленная, в основном, содержанием воды (3-5 для сухой почвы и ~80 для воды), создает принципиальную возможность дистанционного определения влажности [2]. Однако практическая интерпретация данной зависимости связана с существенными трудностями, обусловленными гетерогенным составом почв, вариациями их гранулометрического состава, плотности, засоленности, температуры и др. [3].

В настоящее время существует значительное количество моделей, описывающих связь диэлектрической проницаемости почвы с её влажностью [4-7]. Среди них наибольшее распространение и признание в научном сообществе получили подходы, изложенные в работах [5, 7], которые были выбраны в качестве основных объектов настоящего анализа.

В работе [5] представлено эмпирическое соотношение, известное как формула Топпа и получившее достаточно широкое признание благодаря своей универсальности:

$$\varepsilon_a = 3,03 + 9,3W + 146W^2 - 76,7W^3, \quad (1)$$

где ε_a – кажущаяся диэлектрическая проницаемость; W – влажность почвы.

Уравнение (1) даёт оценку влажности почвы в диапазоне частот 20 МГц – 1 ГГц без учёта температуры, солёности и плотности грунта. Вместе с тем, оно не учитывает физико-химические процессы взаимодействия воды с неоднородной структурой почвы.

Наиболее часто используемой в задачах дистанционного зондирования является полуэмпирическая модель Добсона, представленная в работе [7]:

$$\begin{cases} \varepsilon'_{soil} = [1 + (\rho_b/\rho_s)(\{\varepsilon'_{sm}\}^\alpha - 1) + W_m^{\beta'} (\varepsilon'_{fw})^\alpha - W_m]^{1/\alpha} \\ \varepsilon''_{soil} = [W_m^{\beta''} (\varepsilon''_{fw})^\alpha]^{1/\alpha} \end{cases} \quad (2)$$

где: ε'_{soil} – действительная часть КДП; ε''_{soil} – мнимая часть КДП; W_m – объёмная влажность почвы; ρ_s – плотность сухой фракции почвы; ρ_b – плотность почвы; ε'_{sm} – диэлектрическая проницаемость твердых частиц почвы; α , β' , β'' – константы; ε'_{fw} – действительная часть диэлектрической проницаемости свободной

воды; ε'_{fw} – мнимая часть диэлектрической проницаемости свободной воды; T – температуры ($^{\circ}\text{C}$); P_{sand} – процентное содержание песка; P_{clay} – процентное содержание глины; P_{silt} – процентное содержание ила.

Типичные (опорные) значения процентного содержания составляющих, удельного веса и объемной плотности для четырех типичных типов почвы приведены в [8].

Модель (2) позволяет рассчитать КДП почвы в диапазоне частот 0,3 – 18 ГГц на основе известного гранулометрического состава и плотности почвы. Несмотря на достаточно широкое распространение данной модели, её использование в различных регионах России, имеющих существенные отличия в структурном составе почвы, требует уточнения входных параметров (коэффициентов). При исследовании почв с высоким содержанием органических веществ (например, торфяников) или в условиях их высокой засоленности данная модель требует дополнительных исследований и существенной коррекции входных данных, что негативным образом влияет на точность определения влажности и вычислительную сложность модели.

Расчеты дополнительно осложняются тем, что входящие в (2) действительная и мнимая части диэлектрической проницаемости воды ε'_{fw} , ε''_{fw} связаны с объемной влажностью почвы [8]:

$$\varepsilon'_{fw} = \frac{\varepsilon_s - \varepsilon_1}{1 + \left(\frac{f_{GHz}}{f_1}\right)^2} + \frac{\varepsilon_1 - \varepsilon_{\infty}}{1 + \left(\frac{f_{GHz}}{f_2}\right)^2} + \varepsilon_{\infty} + \frac{18\sigma'_{eff}(p_s - p_b)}{f_{GHz}p_sW_m}, \quad (3)$$

$$\varepsilon''_{fw} = \frac{\left(\frac{f_{GHz}}{f_1}\right)(\varepsilon_s - \varepsilon_1)}{1 + \left(\frac{f_{GHz}}{f_1}\right)^2} + \frac{\left(\frac{f_{GHz}}{f_2}\right)(\varepsilon_1 - \varepsilon_{\infty})}{1 + \left(\frac{f_{GHz}}{f_2}\right)^2} + \frac{18\sigma''_{eff}(p_s - p_b)}{f_{GHz}p_sW_m}, \quad (4)$$

где f_{GHz} – частота зондирующего сигнала (ГГц); ε_s – статическая диэлектрическая проницаемость воды; ε_1 – диэлектрическая проницаемость, соответствующая первой релаксационной области; ε_{∞} – высокочастотная диэлектрическая проницаемость; f_1, f_2 – релаксационные частоты; σ_{eff} – эффективная проводимость.

Поскольку рассмотренные аналитические модели [4-7] носят эмпирический и полуэмпирический характер, они обладают следующими недостатками: в полуэмпирических моделях влажность входит в уравнения нелинейно и неявно, что требует итерационных процедур вычисления, чувствительных к начальному приближению и накоплению численной погрешности, а эмпирические модели не учитывают параметры почвы. Это ведет к неоднозначности интерпретации данных и снижению достоверности оценок влажности.

Целью исследования является разработка модернизированной имитационной модели Добсона, в которой действительная и мнимая части комплексной диэлектрической проницаемости свободной воды ε'_{fw} , ε''_{fw} заменены на действительную и мнимую части комплексной диэлектрической проницаемости связанной воды ε'_{bw} , ε''_{bw} , учитывающие структурную неоднородность влаги в тонких пленках на поверхности минеральных частиц.

Для достижения указанной цели необходимо:

- получить математические выражения для оценки действительной и мнимой частей комплексной диэлектрической проницаемости почвы;
- проверить адекватность полученных выражений.

Для этого используем подход [9], где обоснована возможность использования результатов радиолокационных измерений КДП почвы для определения ее объемной влажности и удельной проводимости. Подход основан на наклонном облучении земной поверхности вертикально и горизонтально поляризованным радиосигналом фиксированной частоты под разными углами падения с последующим приемом интерференционного сигнала в условиях диффузно-зеркального отражения. Действительная и мнимая части КДП определяются с использованием формул Френеля для условий полного (псевдополного) преломления при угле падения, равном углу (псевдоуглу) Брюстера, который фиксируется по возникновению разности фаз между вертикально и горизонтально поляризованными составляющими отраженного интерференционного сигнала. Действительная часть диэлектрической проницаемости почвы в модели определяется как

$$\varepsilon = (tg\varphi_B)^2.$$

Заменим диэлектрическую проницаемость свободной воды ε_{fw} в (2) на диэлектрическую проницаемость связанной воды ε_{bw} , учитывающую структурную неоднородность влаги в тонких пленках на поверхности минеральных частиц. Такая замена является физически обоснованной, поскольку при малых и средних значениях влажности, а также при отрицательных температурах значительная доля почвенной влаги

находится в связанном состоянии, диэлектрические свойства которого существенно отличаются от свойств объемной свободной воды [10]

$$\varepsilon'_{bw} = \varepsilon_{\infty} + \frac{\varepsilon_s - \varepsilon_{\infty}}{1 + \left(\frac{\lambda_{bw}(t)}{\lambda}\right)^2}, \quad (5)$$

$$\varepsilon''_{bw} = \frac{(\varepsilon_s - \varepsilon_{\infty}) \left(\frac{\lambda_{bw}(t)}{\lambda}\right)}{1 + \left(\frac{\lambda_{bw}(t)}{\lambda}\right)^2}, \quad (6)$$

где λ_{bw} – релаксационная длина волны связанной воды; t – температура почвы в градусах; τ_{bw} – релаксации молекул связанной воды.

Время релаксации, зависящее от числа мономолекулярных слоев воды $\tau_{bw}(t)$, определяется по таблице 1 [10].

Таблица 1

Время релаксации в зависимости от числа мономолекулярных слоев

Число мономолекулярных слоев воды	Время релаксации молекул воды $\tau_{bw}(27^{\circ}\text{C})$, с
1	$5,0 * 10^{-10}$
2	$5,0 * 10^{-11}$
4	$2,2 * 10^{-11}$
8-12 (свободная вода)	$7,7 * 10^{-12}$

В работе [10] обосновано, что для большинства типов почв в диапазоне малых и средних влажностей толщина пленки связанной воды соответствует двум мономолекулярным слоям, что принимается в дальнейших расчетах. Окончательные выражения получаются после подстановки выражений (5) и (6) в (2):

$$\begin{cases} \varepsilon'_{soil} = [1 + (\rho_b/\rho_s)(\{\varepsilon'_{sm}\}^{\alpha} - 1) + W_m^{\beta'} (\varepsilon'_{bw})^{\alpha} - W_m]^{1/\alpha} \\ \varepsilon''_{soil} = [W_m^{\beta''} (\varepsilon''_{bw})^{\alpha}]^{1/\alpha} \end{cases} \quad (7)$$

Система уравнений (7) учитывает взаимосвязи между составляющими комплексной диэлектрической проницаемости ε_{soil} и объемной влажностью W_m почвы, зависящей от диэлектрической проницаемости связанной воды ε_{bw} . В отличие от классической модели Добсона, предложенное решение позволяет проводить аналитические расчеты, сводя задачу к определению целевого параметра (влажности почвы) без использования итеративных расчетов [11].

Для оценки точности и адекватности разработанной модели проведена ее валидация на основе сопоставления расчетных значений объемной влажности с результатами её измерений влагомером TDR-150 (Spectrum Technologies, щуп 20 см, точность измерений $\pm 3\%$) [12]. Эксперименты проводились на глинистом суглинке в полевых условиях. Результаты измерений представлены в таблице 2.

Таблица 2

Экспериментальные значения			
Исследования	Значения TDR-150		Угол Брюстера, градусы
	Объемная влажность, %	Удельная проводимость, см/См	
Эксперимент 1	10,0	0,02	67,4809
Эксперимент 2	19,3	0,10	68,9213
Эксперимент 3	31,2	0,19	70,9117
Эксперимент 4	40,6	0,27	72,4798

Полученные значения объемной влажности (в процентах) представлены в виде четырех диаграмм (рисунок 1), каждая из которых соответствует отдельному эксперименту и отражает величину расхождения между опорным значением влажности (TDR-150) и расчетными значениями, полученными по моделям Топпа, Добсона и модифицированной модели Добсона.

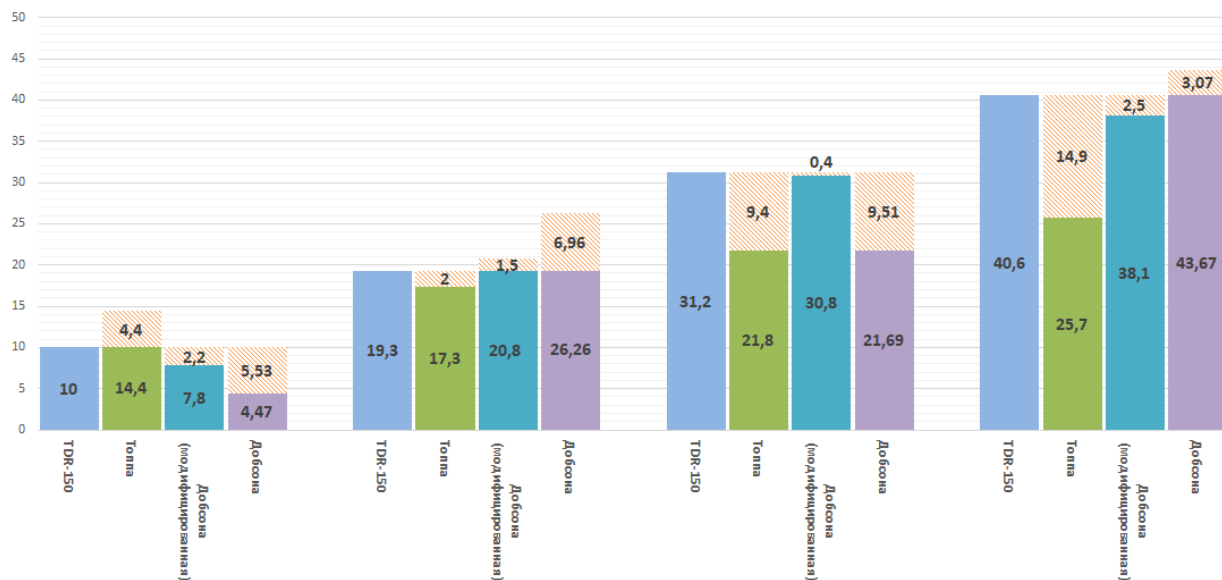


Рисунок 1 – Абсолютная ошибка расчета объемной влажности почвы моделей Топпа [5], Добсона [7] и модифицированной модели Добсона (7) (выделенная штриховкой область – абсолютная ошибка)

Анализ полученных данных позволяет сделать следующие выводы: модель со связанной влажностью (7) демонстрирует наибольшую точность во всем диапазоне исследований, минимальная ошибка составила 0,4 %, максимальная 2,5 %. Классическая модель Добсона показывает удовлетворительные результаты (минимальная ошибка составила 3,07 %, максимальная 9,51 %.), а уравнение Топпа, будучи чисто статистической зависимостью, не учитывает физико-химические показатели, что приводит к значительным отклонениям от значений влагомера TDR-150 (минимальная ошибка составила 2 %, максимальная 14,9 %).

Преимуществами разработанной модели (7) являются:

- упрощение вычислений, что повышает скорость расчетов;
- учет связанной воды через параметры релаксации Дебая;
- адаптивность к конкретным условиям измерений (частота, тип почвы, температурный режим).

Однако при исследовании почв с высоким содержанием органического вещества, при повышенной солености и в условиях шероховатости поверхности почвы, нарушающей условия зеркального отражения радиолокационного сигнала, точность определения объемной влажности несколько снижается, что ограничивает применение разработанной модели в указанных условиях.

Оценка влияния подповерхностной электромагнитной волны на точность разработанной модели и проведение дополнительных экспериментов для других типов почв являются задачами дальнейших исследований.

Работа выполнена в рамках реализации программы стратегического академического лидерства «Приоритет-2030» при финансовой поддержке Минобрнауки России.

Литература

1. Петракова Н. В. Перспективы цифровизации сельского хозяйства в России // Трансформации современного общества: теоретические и практические аспекты: Материалы VII Международной научно-практической конференции, 24–25 апреля. Москва: Московский институт экономики, политики и права. 2025. С. 146–149.
2. Wang R., Souilamas M., Esfandiar A., Fabregas R., Ben S., Nevison-Andrews H., Yang Q., Normansell J., Ares P., Ferrari G., Principi A., Geim A. K., Fumagalli L. In-plane dielectric constant and conductivity of confined water // Nature. 2025. vol. 646(8085), pp. 606–610. [doi: 10.1038/s41586-025-09558-y](https://doi.org/10.1038/s41586-025-09558-y)
3. ГОСТ Р 56157–2014 Методики (методы) анализа состава и свойств проб почв: дата введения 09.10.2014. – Москва: Изд-во Стандартиформ, 2015. – 12 с.
4. De Loor G. P. Dielectric Properties of Heterogeneous Mixtures Containing Water // J. Microwave Power. 1968. vol. 3, pp. 67–73. doi: 10.1080/00222739.1968.11688670.

5. Topp G. C., Davis J. L., Annan A. P. Electromagnetic determination of soil water content: Measurements in coaxial transmission lines // Water resources research. 1980, vol. 16, no. 3, pp. 574–582. doi:10.1029/WR016i003p00574.
6. Wang J. R., Schmugge T. J. An Empirical Model for the Complex Dielectric Permittivity of Soils as a Function of Water Content // IEEE Transactions on Geoscience and remote sensing. 1980. vol. GE-18, no. 4, pp. 288–295. doi: 10.1109/TGRS.1980.350304.
7. Dobson M. C., Ulaby F. T., Hallikainen M. T., El-rayes M. A. Microwave Dielectric Behavior of Wet Soil-Part II: Dielectric Mixing Models // IEEE Transactions on Geoscience and Remote Sensing. 1985. vol. GE-23, no 1, pp. 35-46. doi: 10.1109/TGRS.1985.289498.
8. Рекомендация МСЭ-R P.527 – 4(06/2017). Электрические характеристики земной поверхности. Серия Р. Распространение радиоволн.
9. Линец Г. И., Баженов А. В., Гривенная Н. В., Гончаров В. Д. Радиолокационное измерение комплексной относительной диэлектрической проницаемости и объемной влажности почвы. // Радиоэлектронные устройства и системы для инфокоммуникационных технологий ("РЭУС-ИТ 2023"): Доклады Всероссийской Конференции, Посвящённой "Дню Радио", 07–09 июня. Москва: Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова. 2023. С. 79–83.
10. Боярский Д. А., Тихонов В. В. Влияние связанной воды на диэлектрическую проницаемость влажных и мерзлых почв [М.]: Ин-т косм. исслед. (ИКИ) РАН, 2003. – 47 с.
11. Патент России 2804381С1, Кл. G01N 27/02, опубл. 28.09.2023. Устройство дистанционного измерения влажности плоскостойких диэлектриков с потерями.
12. FieldScout TDR 150 Soil Moisture Meter. Available at: <https://www.specmeters.com/FieldScout-TDR150-Soil-Moisture-Meter-Case-Included> (accessed 15.04.2026).

MODIFIED DOBSON SIMULATION MODEL FOR REMOTE DETERMINATION OF SOIL MOISTURE

Prof., Dr.Sc. Linets G.I., Prof., PhD Bazhenov A.V., Ass. Prof., PhD, Grivennaya N.V.,
Researcher, Malygin S.V., Ass. Prof., PhD, S.V. Melnikov, Student Goncharov V.D.
North Caucasus Federal University, Stavropol 355017, Russia;

The paper presents a modified Dobson model for remote determination of volumetric soil moisture, in which the parameters of free water are replaced by the characteristics of bound water. Analytical formulas are derived that eliminate iterative calculations and allow direct estimation of moisture content from the complex dielectric permittivity. To assess the accuracy and adequacy of the developed model, its validation is carried out by comparing the calculated volumetric moisture values from the developed model, the classical Dobson and Topp models, with measurement results obtained using a TDR-150 moisture meter (Spectrum Technologies, 20 cm probe). The results of the developed model demonstrate the best accuracy over the entire range of the study.



МАТЕМАТИЧЕСКИЕ МОДЕЛИ ОДНОКАНАЛЬНОГО АВТОКОМПЕНСАТОРА ПОМЕХ

Магистр, науч. сотр. Лэ В.Т.¹,
Магистр, преп. Нгуен Д.В.²

¹Технологический институт

²Технический университет имени Ле Куй Дона

В статье приводятся математические модели одноканального автокомпенсатора помех для трех групп алгоритмов работы: *LMS*, *SMI*, *RLS* и их модификаций. В статье математические модели одноканального цифрового автокомпенсатора помех представлены как разновидности математической модели некоторого обобщенного *LMS*-алгоритма. Разновидности математических моделей одноканального автокомпенсатора помех для всех алгоритмов отличаются между собой только коэффициентом сходимости и крутизной дискриминационной характеристики.

Введение

Алгоритмы адаптивной пространственной обработки сигналов делятся на три большие группы [1, 2, 3], сильно отличающиеся формами записи и свойствами:

- алгоритмы, реализующие градиентный метод (*LMS*-алгоритм и его модификации);
- алгоритмы непосредственного обращения матрицы (*SMI*-алгоритмы);
- алгоритмы рекурсивных наименьших квадратов (*RLS*-алгоритмы).

Сильные отличия в форме записи алгоритмов работы одноканального автокомпенсатора помех затрудняет сравнительный анализ их свойств и характеристик. В работе [4] показано, что алгоритмы работы одноканального цифрового автокомпенсатора помех могут быть представлены как разновидности некоторого обобщенного *LMS*-алгоритма. В данной статье рассматривается задача построения математических моделей обобщенного *LMS*-алгоритма.

1 Алгоритмы работы одноканального цифрового автокомпенсатора помех

В работе [4] показано, что алгоритмы работы одноканального цифрового автокомпенсатора помех можно записать в следующем обобщенном виде (рисунок 1):

$$W(n) = W(n-1) - U_{\infty}(n) = W(n-1) - \mu(n) f(E_K(k)) E_K^*(n) E_{\Sigma}(n). \quad (1)$$

Таблица 1.

Алгоритмы работы одноканального автокомпенсатора

Алгоритм	$\mu(n)$	$f(E_K(k))$	$U_{\infty}(n)$
LMS	μ	K_{Π}	$\mu K_{\Pi} E_K^*(n) E_{\Sigma}(n)$
NLMS	μ	$\frac{1}{ E_K(n) ^2}$	$\mu \frac{1}{ E_K(n) ^2} E_K^*(n) E_{\Sigma}(n)$
LMS-Newton	μ	$\frac{1}{\frac{1}{n} \sum_{k=1}^n E_K(k) ^2}$	$\mu \frac{1}{\frac{1}{n} \sum_{k=1}^n E_K(k) ^2} E_K^*(n) E_{\Sigma}(n)$
SMI	$\frac{1}{n}$	$\frac{1}{\frac{1}{n} \sum_{k=1}^n E_K(k) ^2}$	$\frac{1}{n} \frac{1}{\frac{1}{n} \sum_{k=1}^n E_K(k) ^2} E_K^*(n) E_{\Sigma}(n)$
RLS	$\frac{1}{n} \frac{\sum_{k=1}^n E_K(k) ^2}{\sum_{k=1}^n \lambda^{n-k} E_K(k) ^2}$	$\frac{1}{\frac{1}{n} \sum_{k=1}^n E_K(k) ^2}$	$\frac{1}{\sum_{k=1}^n \lambda^{n-k} E_K(k) ^2} E_K^*(n) E_{\Sigma}(n)$

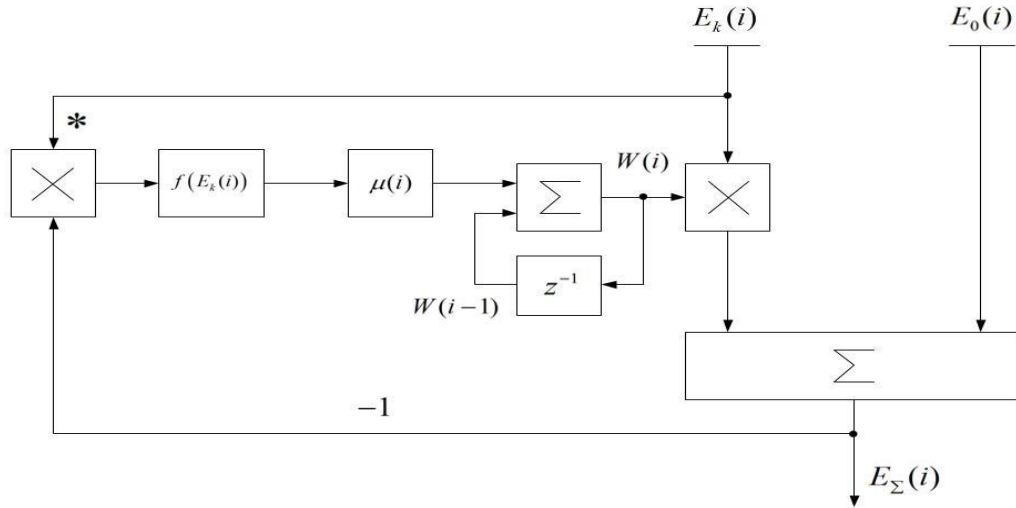


Рисунок 1 – структурная схема обобщенного одноканального автокомпенсатора

2 Математическая модель обобщенного одноканального автокомпенсатора помех

С использованием замены $E_z(n) = E_0(n) + E_K(n) \cdot W(n)$ алгоритм работы обобщенного одноканального цифрового автокомпенсатора помех (1) после преобразований можно записать в следующем виде:

$$W(n) = W(n-1) - \mu(n) f(E_K(k)) E_K^*(n) E_K(n) \left[\frac{E_K^*(n) E_0(n)}{E_K^*(n) E_K(n)} + W(n) \right]. \quad (2)$$

После усреднения по реализациям можно получить следующее уравнение для средних значений весовых коэффициентов:

$$\overline{W(n)} = \overline{W(n-1)} + \mu(n) \cdot K_d \left[W_3(n) - \overline{W(n)} \right], \quad (3)$$

где $W_3(n) = - \frac{\overline{E_K^*(n) E_0(n)}}{\overline{E_K^*(n) E_K(n)}}$;

$2\sigma_k^2 = \overline{E_K^*(n) E_K(n)}$ – мощность сигнала помехи в компенсационном канале;

$K_d \approx \overline{f(E_K(k))} \cdot 2\sigma_k^2$ – крутизна дискриминационной характеристики.

С учетом случайной составляющей сигнала ошибки $U_{co}(n)$ уравнение для весовых коэффициентов примет следующий вид:

$$W(n) = W(n-1) + \mu(n) \cdot K_d \left[W_3(n) - W(n) \right] + \xi(n). \quad (4)$$

Для удобства последующей работы пересчитаем случайную составляющую сигнала ошибки $\xi(n)$ пересчитывают на вход дискриминатора [5]:

$$W(n) = W(n-1) + \mu(n) \cdot K_d \left[W_3(n) - W(n) + \eta(n) \right], \quad (5)$$

где $\eta(t) = \frac{\xi(n)}{\mu(n) \cdot K_d}$ – случайное возмущающее воздействие измерителя.

Полагая сигнал помехи в канале приема гауссовским случайным процессом с нулевым средним, можно получить следующее выражение для корреляционной функции случайного возмущающего воздействия измерителя весового коэффициента в установившемся режиме ($W = W_{зад}$) [5]:

$$R_\eta(\tau) = \overline{\eta(t) \eta^*(t-\tau)} = (1-r^2) r^2(\tau) |W_{зад}|^2, \quad (6)$$

где $r(\tau)$ – нормированная корреляционная функция помехи.

Соответственно, спектральная плотность случайного возмущающего воздействия (ее еще называют эквивалентной спектральной плотностью возмущающего воздействия измерителя) описывается выражением (предполагается, что корреляционная функция помехи описывается экспоненциальной аппроксимацией) [5]:

$$S_{эКВ} = S_\eta = S_\eta(\omega) \Big|_{\omega=0} = \frac{1}{2\pi} \int_{-\infty}^{\infty} R_\eta(\tau) d\tau = \frac{1-r^2}{2\Delta f_{ш}} |W_{зад}|^2. \quad (7)$$

где $\Delta f_{\text{ш}}$ – ширина спектра шумовой помехи.

Задающее воздействие представляет собой требуемое значение весового коэффициента и может быть записано в комплексном виде [5]:

$$W_{\text{зад}} = A_w e^{i\varphi}, \quad (8)$$

где $A_w = \frac{\sigma_0}{\sigma_k} r = \frac{A_{\text{осн}}(\beta_{\text{п}})}{A_{\text{комп}}(\beta_{\text{п}})} r$ – амплитудный множитель задающего воздействия с точностью до знака;

$A_{\text{осн}}(\beta_{\text{п}})$ – значение диаграммы направленности основной антенны в направлении на источник помехи;

$A_{\text{комп}}(\beta_{\text{п}})$ – значение диаграммы направленности компенсационной антенны в направлении на источник помехи;

$\varphi = \frac{2\pi\Delta R}{\lambda}$ – набег фазы сигнала помехи между основным и компенсационным каналами приема.

3 Сравнение алгоритмов для одноканального автокомпенсатора

Таким образом, с учетом изложенного, математическая модель измерителя весового коэффициента обобщенного одноканального автокомпенсатора имеет вид:

$$W(n) = W(n-1) + \mu(n) \cdot K_d [W_{\text{зад}}(n) - W(n) + \eta(n)]. \quad (9)$$

Эквивалентная структурная схема дискретной системы измерения весового коэффициента обобщенного одноканального автокомпенсатора, соответствующая выражению (9), приведена на рисунке 2.

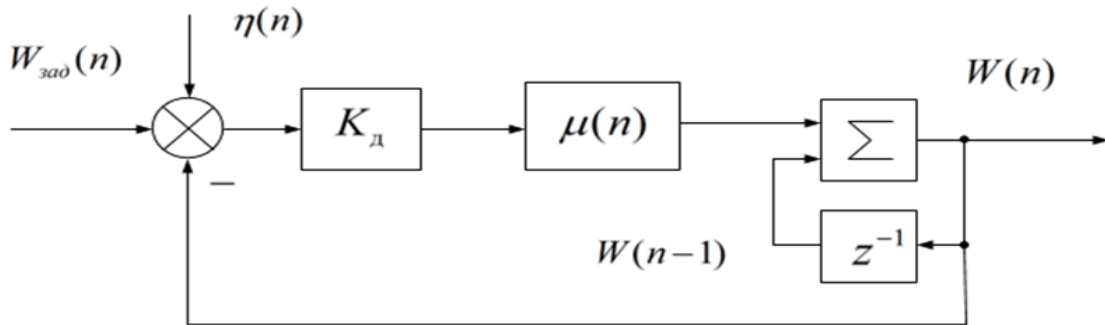


Рисунок 2 – Эквивалентная структурная схема дискретной системы измерителя весового коэффициента

Таблица, в которой представлены все математические модели одноканального автокомпенсатора и его параметры, имеет следующий вид.

Таблица 2.

Математические модели одноканального автокомпенсатора и его параметры

Алгоритм	$\mu(n)$	$K_d = \overline{f(E_k(k))} \cdot 2\sigma_k^2$	$\overline{U_{\text{co}}(n)}$
LMS	μ	$2K_{\text{п}}\sigma_k^2$	$K_d \mu(n) (W_{\text{зад}} - W(n) + \eta(n))$
NLMS	μ	$K_{\text{п}}$	$K_d \mu(n) (W_{\text{зад}} - W(n) + \eta(n))$
LMS-Newton	μ	1	$K_d \mu(n) (W_{\text{зад}} - W(n) + \eta(n))$
SMI	$\frac{1}{n}$	1	$K_d \mu(n) (W_{\text{зад}} - W(n) + \eta(n))$
RLS	$\frac{1-\lambda}{1-\lambda^n}$	1	$K_d \mu(n) (W_{\text{зад}} - W(n) + \eta(n))$

Заключение

Из выражения (9) и Таблицы 2 видно, что все математические модели одноканального автокомпенсатора имеют одинаковую форму записи. Они отличаются между собой только коэффициентом сходимости $\mu(n)$ и крутизной дискриминационной характеристики.

Литература

1. Монзинго Р.А., Миллер Т.У. Адаптивные антенные решетки / М.: Радио и связь, 1986. 446 с.
2. Aurelio Uncini. Fundamentals of Adaptive Signal Processing / Springer, 2015. 704 p.
3. Джиган В.И. Адаптивная фильтрация сигналов: теория и алгоритмы / Москва: Техносфера, 2013. 528 с.
4. Д. В. Нгуен, И. Н. Давыденко Эквивалентная форма записи алгоритмов работы одноканального автокомпенсатора помех, Доклады 24-й международной конференции "DSPA", 2022 – С. 96-100.
5. Костромицкий, С. М. Вопросы радиоавтоматики адаптивных антенных решеток / С. М. Костромицкий, И. Н. Давыденко: Нац. Акад. наук Беларуси, Центр радиотехники. – Минск, 2021. С 174с.
6. Костромицкий, С. М. Сравнительный анализ эффективности одноканальных автокомпенсаторов непрерывных шумовых помех / С. М. Костромицкий, Д. В. Нгуен, И. Н. Давыденко // Базис, 2020. – №2(8). – С. 50-57.

MATHEMATICAL MODELS OF ONE-CHANNEL CANCELLER OF JAMMER

Master, Researcher Le V.T¹, Master, Nguen D.V¹.

¹Technological Institute, Ha Noi, VietNam

²Le Quy Don Technical University, Ha Noi, VietNam

The article presents mathematical models of one-channel canceller of jammer for three groups of operational algorithms: LMS, SMI, RLS, and their modifications. In the article, the mathematical models of the single-channel digital interference canceller are represented as variants of a mathematical model of a certain generalized LMS algorithm. The variations of the mathematical models for all algorithms differ from one another only in their convergence coefficient and the steepness of the discrimination characteristic.



МЕТОДЫ ФОРМИРОВАНИЯ ПРОСТРАНСТВЕННОГО МИНИМУМА ИЗЛУЧЕНИЯ В РЛС С ПРОСТРАНСТВЕННО-ВРЕМЕННОЙ МОДУЛЯЦИЕЙ ЗОНДИРУЮЩЕГО СИГНАЛА НА ОСНОВЕ ФУНКЦИЙ УОЛША

проф. Кутузов В. М., асп. Май Т. З.

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

В докладе рассматриваются методы управления пространственными энергетическими характеристиками работы когерентной РЛС с эквидистантной плоской антенной решеткой при использовании пространственно-временной модуляции зондирующего сигнала на основе кодов Уолша. Рассматриваются два альтернативных метода, один из которых основан на дополнительной противофазной манипуляции в антенной решетке от элемента к элементу, а другой использует дополнительные весовые коэффициенты для каждого антенного элемента. Показано, что использование предлагаемых методов позволяет ослабить излучение зондирующего сигнала в заданном направлении, но при этом уровень ослабления полезного сигнала зависит от углового расстояния между заданным направлением и лоцируемым объектом. В заключении приведено сравнение энергетической скрытности работы РЛС при использовании рассматриваемых методов при различных условиях работы энергетического приемника.

Конфликт между высокой мощностью излучения, необходимой для повышения эффективности обнаружения цели, и необходимостью ее снижения для обеспечения скрытности работы радиолокационных систем (РЛС) по-прежнему является проблемой при проектировании современных РЛС. Традиционный подход основан на применении сложно модулированных широкополосных сигналов с большой базой, которая определяется как произведение эффективной длительности когерентного сигнала на его эффективную полосу спектра. Для повышения информационной (структурной) скрытности используют шумоподобные сигналы с фазокодовой модуляцией на основе псевдослучайных последовательностей, которые по корреляционным свойствам близки к естественным шумам [1]. Однако для современных высокочувствительных приемников радиомониторинга только снижения пиковой мощности недостаточно для обеспечения скрытности работы РЛС. В данном случае использование РЛС с фазированной антенной решеткой (ФАР), диаграмма направленности (ДН) которой позволяет подавлять излучаемую мощность в направлении энергетического приемника (ЭП), является более эффективным решением.

В исследованиях [2, 3] были предложены два метода формирования пространственного минимума излучения. Первый основан на использовании дополнительной противофазной манипуляции в антенной решетке от элемента к элементу, а второй – на добавлении весовых коэффициентов на каждый антенный элемент (АЭ). Ниже производится сравнение энергетической скрытности РЛС при использовании этих методов в различных условиях работы.

Плоская ФАР размерностью $N \times M$ используется с зондирующими сигналами, имеющими пространственно-временную модуляцию на основе функций Уолша (ФУ) размерностью $N \times M$. При этом каждый АЭ излучает отдельный троичный сигнал вида $\{+1, -1, 0\}$, где $\{+1, -1\}$ задает бинарную фазовую манипуляцию $\{0, \pi\}$ в зависимости от кода ФУ, а $\{0\}$ соответствует режиму приема в приемопередающем АЭ. Обозначим ФУ как $Z_1, Z_2, \dots, Z_{N \times M}$, которые образованы как строки порождающей матрицы Адамара размерностью $(N \times M) \times (N \times M)$. Зондирующий сигнал модулируется на основе пространственно-временной матрицы, схематично представленной ниже в трехмерном виде, в которой две пространственные координаты, определяющие положение АЭ, дополнены третьей координатой времени, характеризующей очередность излучения ФУ:

$$\begin{pmatrix} A_{Э,1,1} & A_{Э,1,2} & \dots & A_{Э,1,M} \\ A_{Э,2,1} & A_{Э,2,2} & \dots & A_{Э,2,M} \\ \dots & \dots & \dots & \dots \\ A_{Э,N,1} & A_{Э,N,2} & \dots & A_{Э,N,M} \end{pmatrix} \Leftrightarrow \begin{pmatrix} Z_1 Z_2 \dots Z_{NM} & Z_2 Z_3 \dots Z_1 & \dots & Z_M Z_{M+1} \dots Z_{M-1} \\ Z_{M+1} Z_{M+2} \dots Z_M & Z_{(n-1)M+m} & \dots & Z_{2M} Z_{2M+1} \dots Z_{2M-1} \\ \dots & \dots & \dots & \dots \\ Z_{NM-M+1} Z_{NM-M+2} \dots Z_{NM-M} & Z_{NM-M+2} Z_{NM-M+3} \dots Z_{NM-M+1} & \dots & Z_{NM} Z_1 \dots Z_{NM-1} \end{pmatrix}$$

Тогда комплексный сигнал, излучаемый $A_{Э,n,m}$, может быть представлен в следующем виде:

$$S_{n,m}(t) = \dot{A}_{n,m}(t) e^{j(2\pi f_0 t + \varphi_{0,n,m})} = A_{n,m}(t) e^{j\varphi_{n,m}(t)} e^{j(2\pi f_0 t + \varphi_{0,n,m})},$$

где: $\dot{A}_{n,m}(t)$ – комплексная амплитуда сигнала $A\dot{E}_{n,m}$; $A_{n,m}(t): \{0, 1\}$ – закон амплитудного кодирования, определяющий режим работы антенны; $\phi_{n,m}: \{0, \pi\}$ – закон фазового кодирования на основе ФУ; $\varphi_{0,n,m}$ – начальная фаза $A\dot{E}_{n,m}$.

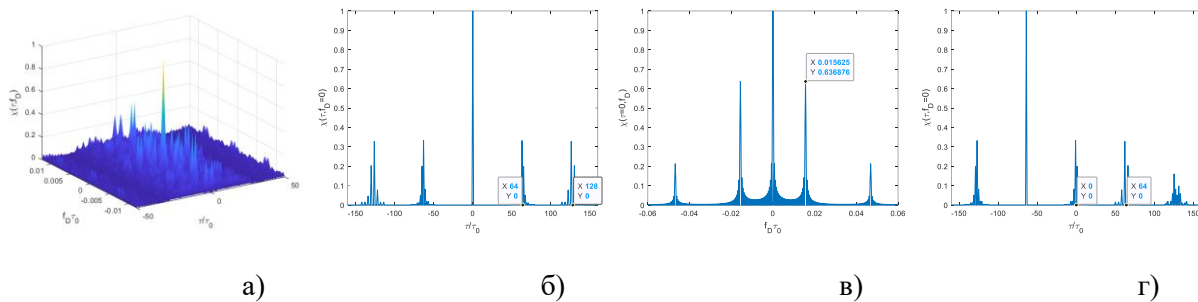


Рисунок 1. Нормированная ФН (а), АКФ (б), СПМ (в) и ВКФ (г) сигналов на основе ФУ 32×32 со скважностью $Q = 2$

Функция неопределенности (ФН) после выполнения согласованной обработки полезного сигнала показана на рисунке 1 (а). Ее сечения при $f_D = 0$ и $\tau = 0$ представляют собой автокорреляционную функцию (АКФ) и спектральную плотность мощности (СПМ) сигнала соответственно. Зависимости на рисунке 1 (б) и (в) иллюстрируют разрешение по задержке (дальности) и доплеровской частоте (скорости) в соответствующих рабочих зонах. Кроме того, ортогональность ФУ (произведение любой пары строк или столбцов матрицы Адамара равно нулю) позволяет строить на основе ФУ ортогональные сигналы, что снижает взаимное влияние сигналов, принимаемых отдельными АЭ ФАР, и повышает точность формирования ДН в режиме приема. Как показано на рисунке 1 (г), в моменты времени, кратные периоду сигнала развязки приема и передачи, значение взаимной корреляционной функции (ВКФ) для любой пары АЭ равно нулю.

При размещении начала декартовой системы координат в положении $A\dot{E}_{1,1}$, пространственную составляющую комплексного сигнала $A\dot{E}_{n,m}$ запишем в виде:

$$S_{n,m}(t - \tau) = \dot{A}_{n,m}(t - \tau) e^{j[2\pi(f_0 + f_D)(t - \tau) + \varphi_{0,n,m}]} e^{j\frac{2\pi}{\lambda}d(n-1)(\sin\theta\sin\phi - \sin\theta_0\sin\phi_0)} e^{j\frac{2\pi}{\lambda}d(m-1)(\sin\theta\cos\phi - \sin\theta_0\cos\phi_0)} \quad (1)$$

где: d – расстояние между соседними АЭ; θ – азимутальный угол; ϕ – угол наклона; θ_0, ϕ_0 – углы отклонения главного лепестка ДН ФАР.

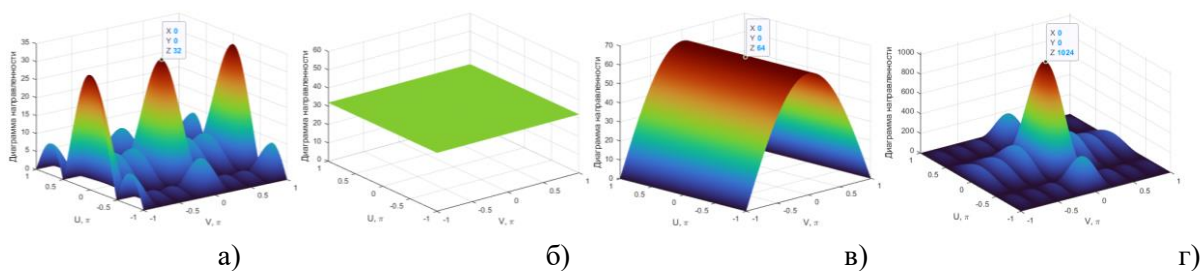


Рисунок 2. Азимутальные зависимости накопления сигналов, излучаемых плоской ФАР 4×8 на основе ФУ 32×32 при суммировании первых: (а) – 2 чипа; (б) – 32 чипа; (в) – 64 чипа; г – 1024 чипа

Для удобства дальнейшего анализа введем нормированные пространственные частоты: $U = \pi \sin \theta \sin \phi$, $V = \pi \sin \theta \cos \phi$, и $d = \lambda/2$, тогда (1) имеет вид:

$$S_{n,m}(t - \tau) = \dot{A}_{n,m}(t - \tau) e^{j[2\pi(f_0 + f_D)(t - \tau) + \varphi_{0,n,m}]} e^{j(n-1)(U - U_0)} e^{j(m-1)(V - V_0)}.$$

При накоплении в ЭП в течение K чипов сигнал может быть записан в виде суммы:

$$F_K(U, V) = \sum_{k=1}^K \sum_{n=1}^N \sum_{m=1}^M \dot{A}_{n,m}(k) e^{j[2\pi(f_0 + f_D)(t - \tau) + \varphi_{0,n,m}]} e^{j(n-1)(U - U_0)} e^{j(m-1)(V - V_0)}. \quad (2)$$

Благодаря свойствам ФУ, на рисунке 2 видно, что при короткого времени анализа (накопления) обеспечивается выигрыш в скрытности системы ($K = 2, 32, 64$). Однако при длительном времени анализа (за время полного цикла Уолша, $K = 1024$) преимущество пространственно-временной модуляции исчезает, и азимутальные зависимости накопленных комплексных амплитуд сигналов приближаются к виду, характерному для традиционной РЛС с ФАР. Этот недостаток можно устранить первым методом, заключающимся в добавлении случайного набора начальных фаз для подавления излучения в направлении ЭП. После этого разделения ФАР на подрешетки размером 2×2 и использования для всех пар в этих подрешетках противофазных весовых коэффициентов с единичной амплитудой по направлениям U и V (3):

	V			
	φ	$\varphi + \pi$	$\dots$	
U	$\varphi + \pi$	φ	$\dots$	
	$\dots$	$\dots$	$\dots$	

(3)

Азимутальные зависимости накопленных комплексных амплитуд сигналов для плоской ФАР размером 4×8 на основе ФУ 32×32 были смоделированы в среде MATLAB. Цель при этом располагалась в направлении $U_0 = 0, V_0 = 0$. На рисунках 3 (а), 3 (б) и 4 (а), 4 (б) приведено моделирование азимутальных зависимостей накопленных комплексных амплитуд сигналов за время полного цикла Уолша ($K = 1024$) для двух случаев: при большом ($U_{\text{ЭП}} = \pi/4, V_{\text{ЭП}} = \pi/4$) и малом ($U_{\text{ЭП}} = \pi/32, V_{\text{ЭП}} = \pi/32$) угловом разноразносе между целью и ЭП. Легко заметить, что зона невидимости РЛС при использовании данного метода достаточно широка. При большом угловом разноразносе излучаемая мощность по-прежнему обеспечивает обнаружение цели. Однако когда цель и ЭП находятся ближе друг к другу, резкое снижение излучаемой мощности в направлении цели является существенным недостатком, ограничивающим возможность работы РЛС. Хотя данную задачу можно решить путем «сужения» ДН за счет увеличения расстояния между АЭ решетки, это также означает необходимость решения проблемы неоднозначности либо уменьшения сектора рабочих углов РЛС [4].

Вышеуказанную проблему можно решить, используя второй метод – формирование нулевого излучения в РЛС путем введения весовых коэффициентов для АЭ таким образом, чтобы искомая ДН в режиме передачи имела вид:

$$F_{\Sigma}(U, V) = F_0(U, V) - F_{\text{ЭП}}(U, V) \frac{F_0(U_{\text{ЭП}}, V_{\text{ЭП}})}{F_{\text{ЭП}}(U_{\text{ЭП}}, V_{\text{ЭП}})}.$$

При этом $F_0(U, V)$ и $F_{\text{ЭП}}(U, V)$ являются угловыми зависимостями (2) при просмотре пространственной частоты цели (U_0, V_0) и угловой частоты ЭП ($U_{\text{ЭП}}, V_{\text{ЭП}}$) соответственно. Как видно из рисунков 3 (в), 3 (г) и 4 (в), 4 (г), второй вариант обеспечивает высокую мощность в направлении цели при сохранении нулевого значения излучения в направлении ЭП. Однако после подробного анализа угловых зависимостей сигнала с пространственно-временной модуляцией, основанной на добавлении весовых коэффициентов на каждый АЭ, наблюдается регулярный лепестковый характер, который усиливается с ростом числа АЭ. Это может негативно сказываться на скрытности при использовании сканирующих по углу ЭП.

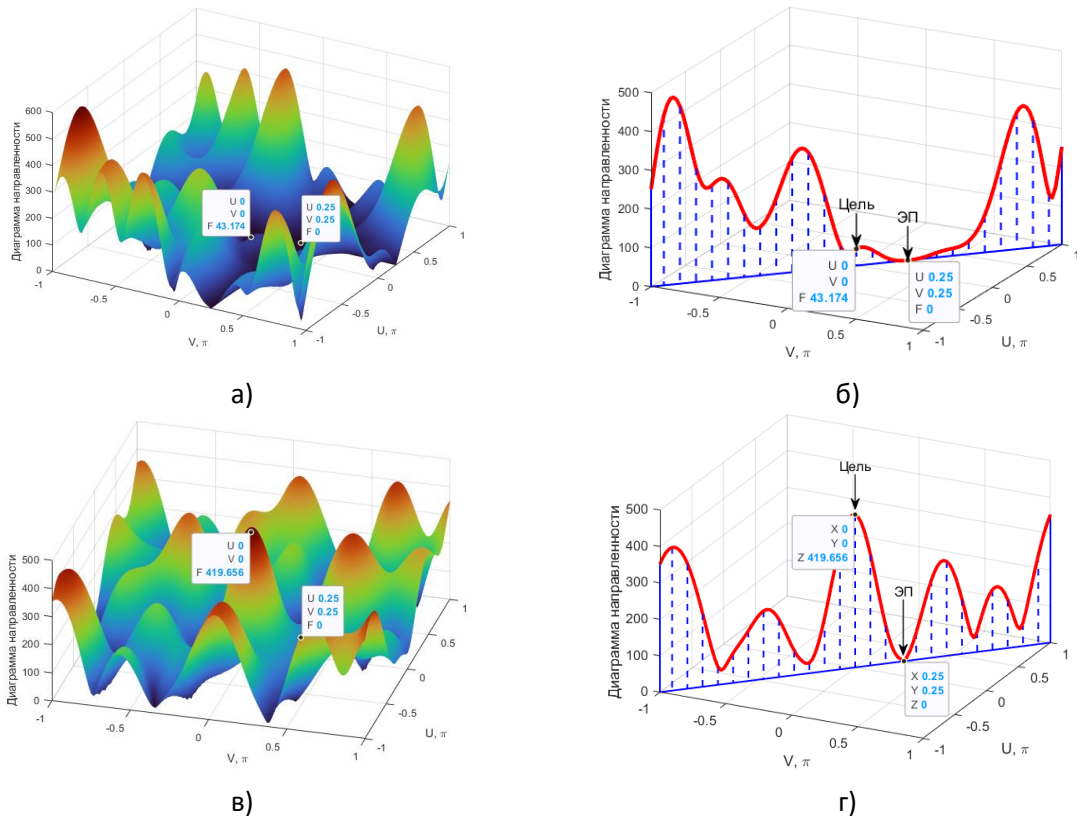


Рисунок 3. Азимутальные зависимости накопленных комплексных амплитуд сигналов ФАР и их сечения плоскостью, проходящей через цель и ЭП, при $U_{ЭП} = \pi/4, V_{ЭП} = \pi/4$:
 а, б – с инверсными фазами АЭ; в, г – с использованием весовых коэффициентов АЭ

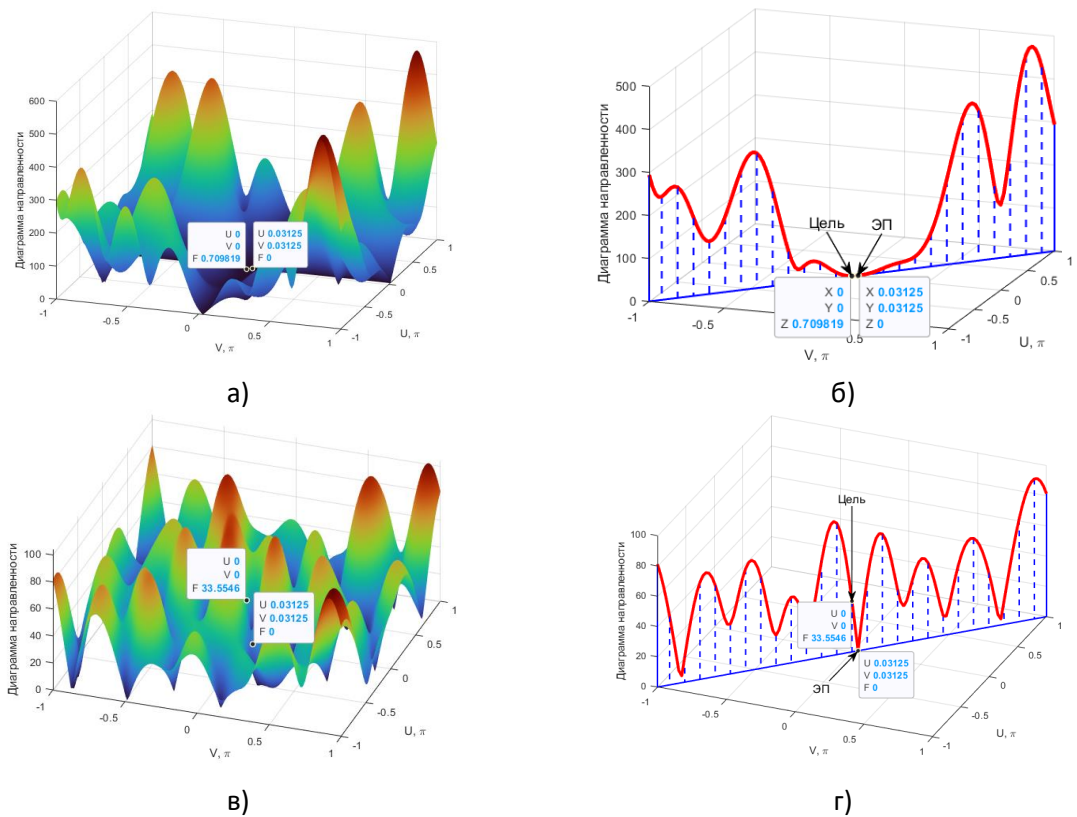


Рисунок 4. Азимутальные зависимости накопленных комплексных амплитуд сигналов ФАР и их сечения плоскостью, проходящей через цель и ЭП, при $U_{ЭП} = \pi/32, V_{ЭП} = \pi/32$:
 а, б – с инверсными фазами АЭ; в, г – с использованием весовых коэффициентов АЭ

Два рассмотренных метода формирования минимума излучения в заданном направлении имеют свои плюсы и минусы. Первый отличается простотой формирования и обработки пространственно-временного сигнала. Весовые коэффициенты в этом случае имеют единичную амплитуду, а фазовые сдвиги, равные 180° и обеспечивающие противофазность, необходимы только половине АЭ, например, четных. Заметим, что при использовании ансамбля ФУ количество АЭ $M \times N$ должно быть четным. При этом область по угловым координатам вблизи направления на ЭП имеет существенные потери в энергии сигнала, облучающего цель. Примеры оценки этих потерь приведен на рисунках 3, б и 4, б. Второй метод приводит к комплексным весовым коэффициентам для всех АЭ, которые применяются при излучении сигнала и в сопряженном виде при пространственно-временной обработке отраженных сигналов. Не смотря на усложнение, второй метод обеспечивает существенно меньшую пространственную область с энергетическими потерями сигнала в направлении на цель, что наглядно иллюстрируют рисунки 3, г и 4, г. Однако, комплексные весовые коэффициенты с разными модулями могут приводить к трансформации совокупного пространственно-временного сигнала, что проявляется в росте боковых лепестков ФН. Предложенная в [3] технология устранения этого эффекта приводит к некоторым дополнительным потерям, что необходимо учитывать при выборе метода.

Литература

1. Кутузов В.М. Работы ЛЭТИ в области скрытной радиолокации // Сборник докладов Всероссийской конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий (РЭУС-ИТ 2025)» – Москва, 22–23 мая 2025 г. – С. 91–95.
2. Кутузов В.М., Май Тунг Зыонг, Жан-Бертранд Баражегетера. Пространственно-временная модуляция зондирующего сигнала на основе функций Уолша в РЛС с ФАР // Сборник докладов Всероссийской научно-практической конференции «Мультимодальные технологии мониторинга и телекоммуникаций (МТМТ'25)» – СПбГЭТУ «ЛЭТИ», Санкт-Петербург, 01 – 03 октября 2025 г. – С. 29-34.
3. Ипатов В.П., Кутузов В.М., Овчинников М.А. Пространственно-частотная модуляция зондирующих сигналов РЛС с ФАР. // Изв. вузов России. Радиоэлектроника. 2025. Т. 28, №4. С. 85–102.
4. Бархатов А.В., Безуглов А.В., Веремьев В.И., Коновалов А.А., Кутузов В.М. Основы проектирования многопозиционных декаметровых РЛС пространственной волны // Под ред. В. М. Кутузова. СПб.: Изд-во СПбГЭТУ "ЛЭТИ", 2012. 191 с.

METHODS FOR FORMING A SPATIAL RADIATION MINIMUM IN RADAR WITH SPACE-TIME MODULATION OF THE PROBING SIGNAL BASED ON WALSH FUNCTIONS

Prof. Vladimir M. Kutuzov, Asp. Mai Tung Duong

Saint Petersburg Electrotechnical University

The paper discusses methods for controlling the spatial energy characteristics of a coherent radar system with an equidistant planar antenna array using space-time modulation of the probing signal based on Walsh codes. Two alternative methods are considered, the first is based on additional anti-phase manipulation within the antenna array from element to element, and the second employs additional weighting coefficients for each antenna element. It is shown that the use of the proposed methods makes it possible to attenuate the radiation of the probing signal in a given direction. However, the level of attenuation of the useful signal depends on the angular separation between the given direction and the target. In conclusion, a comparison is made of the energy stealth performance of the radar system when applying the methods under consideration under various operating conditions of the energy receiver.



ОБНАРУЖЕНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ПРИ ИСПОЛЬЗОВАНИИ ДИСКРЕТНО-МОДУЛИРОВАННЫХ ПО ЧАСТОТЕ СИГНАЛОВ (ДМЧС) И СИСТЕМ ДМЧС (СДМЧС)

к.т.н., преп., Нгуен Тхань Хынг

Технический университет Ле Куи Дон, Вьетнам

В данной статье рассматривается задача радиолокационного обнаружения беспилотных летательных аппаратов (БПЛА) с использованием дискретно-модулированных по частоте сигналов (ДМЧС) и соответствующих систем (СДМЧС). Приводятся особенности формирования и обработки ДМЧС, а также их преимущества при обнаружении малоаметных и маневрирующих целей в условиях интенсивных помех. Показано, что благодаря высокой разрешающей способности по дальности и устойчивости к помехам, сигналы данного типа обеспечивают высокую вероятность обнаружения БПЛА при низком уровне ложных тревог. Приведены результаты численного моделирования, подтверждающие эффективность предложенного подхода в сравнении с традиционными непрерывно-модулированными сигналами.

Введение

Одним из методов повышения эффективности обнаружения беспилотных летательных аппаратов (БПЛА) является увеличение энергетического потенциала РЛС путем наращивания мощности излучения зондирующих сигналов. Однако этот метод является невыгодным [3], [5]. Для решения этой проблемы наиболее целесообразным является использование широкополосных зондирующих сигналов, позволяющих повысить энергетические характеристики РЛС при сохранении высокой разрешающей способности по задержке и частоте, хорошую помехоустойчивость и помехозащищенность, энергетическую скрытность и структурную скрытность, высокую точность синхронизации [1], [6].

Математическая модель систем с использованием дискретно-модулированных по частоте сигналов (ДМЧС)

В связи с этим и для удовлетворения требований, предъявляемых к тактическим параметрам современных РЛС, представляют интерес широкополосные сигналы с большим коэффициентом сжатия, позволяющие получить тела функции неопределенности (ФН) "кнопочного" вида и обеспечивающие одновременную высокую разрешающую способность по времени и частоте, а также низкий УБЛ пьедестала трехмерного тела ФН [2]. Наиболее близкой к требуемой обладает ФН "кнопочного" вида дискретно-модулированных по частоте сигналов (ДМЧС) матрицей Костаса (рис. 1,а, b).

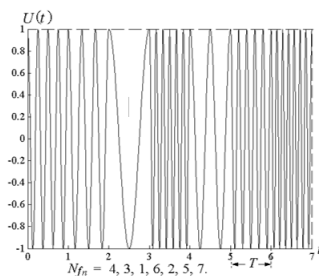


Рисунок 1,а. Комплексная огибающая амплитуда ДМЧС матрицей Костаса с размерностью $N = 7$.

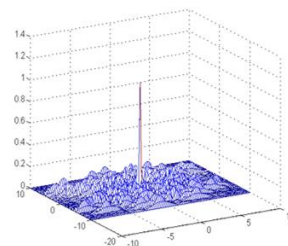


Рисунок 1,б. Тело ФН "кнопочного" вида ДМЧС матрицей Костаса.

Однако увеличение размерности сигнала N приводит к возрастанию трудностей технической реализации при формировании и обработке ДМЧС. Для преодоления указанных трудностей предлагается использовать систему ДМЧС (СДМЧС), представляющую составной сигнал, включающий в себя последовательность из нескольких ДМЧС одинаковой размерности N , но отличающихся порядком изменения дискретных числовых значений частоты. Такие последовательности ДМЧС (ПДМЧС) (рис. 2) и дискретные составные частотные сигналы с частотной манипуляцией (ДСЧЧМ), состоящие из L отдельных ДМЧС имеют общую размерность LN (рис. 3) [4].

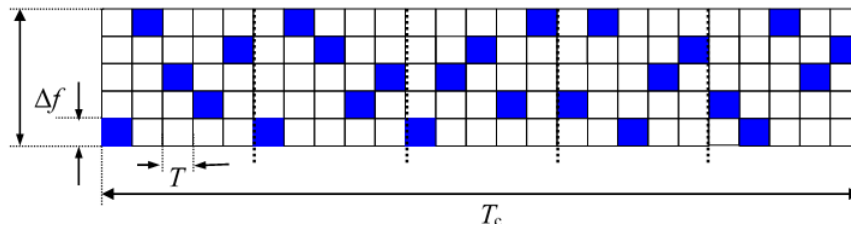


Рисунок 2. Плоскость время-частота для ПДМЧС с размерностью ДМЧС $N = 5$ и количеством ДМЧС $L = 5$.

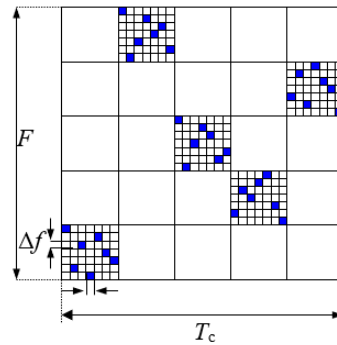


Рисунок 3. Плоскость время-частота для ДСЧЧМ с размерностью $N = 7$ и количеством ДМЧС $L = 5$

Для повышения помехозащищенности и скрытности работы РЛС за счет смены зондирующего сигнала необходимо использовать многоканальный по частоте управляемый фильтр сжатия (УФС) принятого ДМЧС (рисунок 4). ФС для ДМЧС (СДМЧС) может быть построен на основе N полосовых фильтров (ПФ), выходные сигналы которых задерживаются в соответствии с частотно-временной матрицей сигнала и суммируются с учетом начальной фазы элементарных импульсов, где N - размерность ДМЧС (СДМЧС). Каждый ПФ согласован с отдельным элементом сигнала: радиоимпульсом с частотой f_n и имеет полосу пропускания $\Delta f_{\text{пф}}$ равную $1/T$, где T - длительность элементарного радиоимпульса. Сигналы с выхода ПФ поступают в блок весовой обработки (БВО). Блок задержек (БЗ) содержит $(N - 1)$ линий задержек с соответствующей задержкой. Для построения УФС необходимо между набором БВО и БЗ установить управляемый коммутатор (УК), соединяющий выходы БВО с входами линий задержек обеспечивающих формирование в сумматоре требуемого кода частоты ДМЧС (СДМЧС).

Двоичный управляющий код для УК вырабатывается цифровым блоком управления (ЦБУ) в соответствии с частотно-временной матрицей используемого сигнала, который позволяет обрабатывать любой ДМЧС и ПДМЧС с разными кодами частоты и размерностью N меньшей или равной количеству ПФ $N_{\text{ф}}$ на одном ФС. Сигналы с выхода линий задержек суммируются с помощью сумматора. Далее сигналы поступают в накопитель пачки (НП) импульсов. С выхода НП сигнал поступает на пороговое устройство (ПУ), где осуществляется сравнение сигнала с порогом $q_{\text{пор.}}$, в результате которого выносятся решение о наличии или отсутствии полезного сигнала.

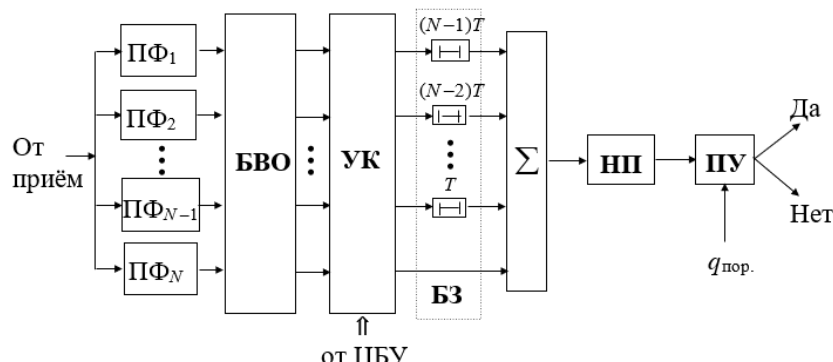


Рисунок 4. Устройство обнаружения БПЛА импульсной когерентной РЛС при использовании ДМЧС.

При обнаружении БПЛА в соответствии со схемой рис. 4 после накопления пачки в НП, сигнал и шум (помеха) поступают на ПУ. Определим отношение сигнал/шум (помеха) по мощности на входе ПУ (выходе НП) для ДМЧС (СДМЧС):

$$q_{\text{с/ш(п)}}^2_{\text{вых.НП}} = q_{\text{с/ш(п)}}^2_{\text{вых.ФС}} n, \quad (1)$$

где n — число импульсов в пачке.

Считая, что равномерный спектр воздействующих помех в полосе пропускания ФС вероятности ложной тревоги F и правильного обнаружения D для детерминированного сигнала при наличии шумов и воздействующих помех можно рассчитать по формулам:

$$F = 1 - \Phi(q_{\text{пор.}}), \quad D = 1 - \Phi(q_{\text{пор.}} - \sqrt{q_{\text{с/ш(п)}}^2}_{\text{вых.НП}}) \quad (2)$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x \exp(-\frac{y^2}{2}) dy = \frac{1}{2} \left(1 + \operatorname{erf}\left(\frac{x}{\sqrt{2}}\right) \right)$ — интеграл вероятностей, $q_{\text{с/ш(п)}}^2_{\text{вых.НП}}$ — отношение сигнал/шум (помеха) на выходе НП.

3.2.1. Но на практике обычно неизвестна начальная фаза и амплитуда сигнала. В этом случае используется модель сигнала со случайными начальной фазой, распределенной по равномерному закону, и амплитудой, распределенной по закону Релея. Для этой модели имеем

$$D = F \frac{1}{1 + \left(\frac{q_{\text{с/ш(п)}}^2_{\text{вых.НП}}}{2} \right)} \quad (3)$$

Если на входе обнаружителя рис. 4 присутствуют сигнал $U(t)$ и собственные шумы приемного тракта (белый шум) с постоянной спектральной плотностью мощности (СПМ) N_0 , то отношение сигнал/шум по мощности на выходе ФС

$$q_{\text{с/ш}}^2_{\text{вых.ФС}} = \frac{2E}{N_0} = \frac{2P_{\text{с вх.ФС}} T_c}{P_{\text{ш}}/F} = \frac{2P_{\text{с вх.ФС}} T_c F}{P_{\text{ш}}} \quad (4)$$

где $E = P_{\text{с вх.ФС}} T_c$ - энергия ДМЧС (СДМЧС), $P_{\text{с вх.ФС}}$ - средняя мощность ДМЧС (СДМЧС) на входе ФС; T_c - длительность ДМЧС (СДМЧС); F - ширина спектра ДМЧС (СДМЧС), $P_{\text{ш}}$ - мощность шума на входе ФС.

Для ДМЧС (СДМЧС) при $M = \Delta f T = 1$ имеем

$$q_{\text{с/ш}}^2_{\text{вых.ФС}} = \frac{2P_{\text{с вх.ФС}} T_c F}{P_{\text{ш}}} = 2B q_{\text{с/ш}}^2_{\text{вх.}} \quad (5)$$

где для ДМЧС $F = N \Delta f$, $T_c = N T$, база $B = F T_c = N \Delta f N T = N^2$, $q_{\text{с/ш}}^2_{\text{вх.}} = \frac{P_{\text{с вх.ФС}}}{P_{\text{ш}}}$ - отношение сигнал/шум по мощности на входе ФС, для ПДМЧС $F = N \Delta f$, $T_c = L N T$, база $B = F T_c = N \Delta f L N T = L N^2$, для ДСЧЧМ $F = L N \Delta f$, $T_c = L N T$, база $B = F T_c = L N \Delta f L N T = L^2 N^2$, L - количество ДМЧС, составляющих ПДМЧС или ДСЧЧМ.

Результат моделирование

3.2.2. В данной работе результат моделирования выполнен с использованием программного обеспечения MATLAB, с применением многоканальной модели сигнала и фильтра сжатия для оценки вероятности обнаружения сигналов типов ДМЧС, ПДМЧС и ДСЧЧМ в условиях помех. В соответствии с (5) следует, что отношение сигнал/шум по мощности на выходе ФС возрастает по сравнению с отношением сигнал/шум на его входе в $2B$ раз, что позволяет значительно повысить энергетические возможности РЛС.

С использованием формул (2), (3) и (5) проведен расчет зависимости вероятности правильного обнаружения D детерминированного сигнала и сигнала со случайными начальной фазой и амплитудой от отношения сигнал/шум (помеха) на входе ФС $q_{\text{с/ш(п)}}^2_{\text{вх.}}$ для ДМЧС с различными размерностями $N = 10, N = 20, N = 30$, вероятностью ложной тревоги $F = 10^{-6}$, некогерентным накоплением числа импульса в пачке $n = 16$, уровнем пьедестала весовой обработки $p = 0,6$, результаты которого представлены на рисунке 5.

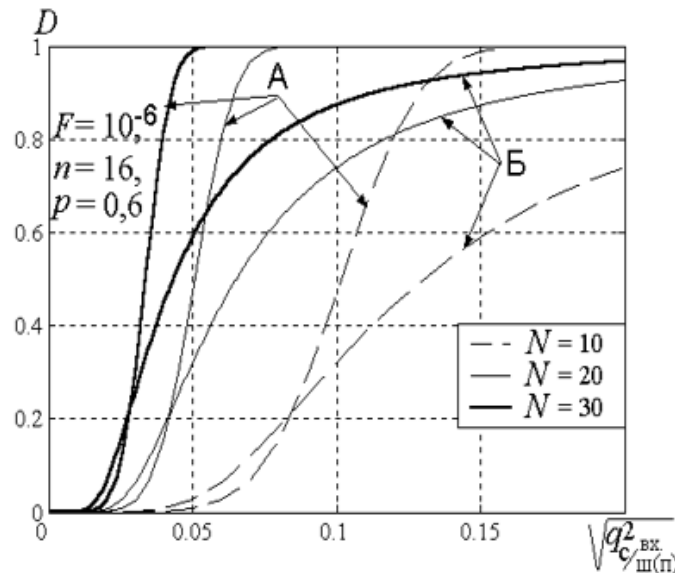


Рисунок 5. Характеристики обнаружения детерминированного сигнала (А) и сигнала со случайными начальной фазой и амплитудой (Б) для различных размерностей ДМЧС при наличии шумов и воздействующих помех с ограниченной мощностью.

В соответствии с результатами расчета видно увеличение вероятности правильного обнаружения D с увеличением размерности сигнала N . При фиксированной вероятности D и увеличении размерности N с 10 до 30, отношение сигнал / шум (помеха) на входе ФС уменьшается в 3 раза. Для обнаружения сигнала со случайными амплитудой и начальной фазой требуется значительно большее отношение сигнал / шум (помеха) на входе ФС, чем для обнаружения детерминированного сигнала (для большой D).

На рисунке 6 показаны графики зависимости D от отношения сигнал / шум (помеха) $q_{c/ш(п)}^2$ на входе ФС для ДМЧС, ПДМЧС и ДСЧЧМ с размерностью $N = 10$ и количеством ДМЧС $L = 5$, $n = 16$, $F = 10^{-6}$, $p = 0,6$.

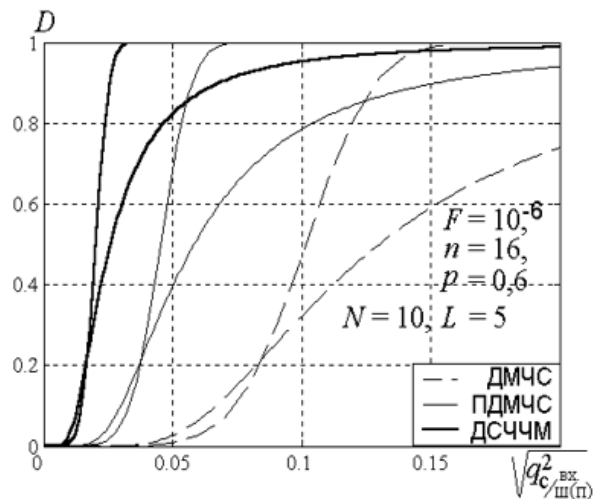


Рисунок 6. Характеристики обнаружения для ДМЧС, ПДМЧС и ДСЧЧМ при наличии шумов и воздействующих помех.

При фиксированных размерности N и количестве ДМЧС L вероятности правильного обнаружения ДСЧЧМ и ПДМЧС увеличиваются по сравнению с ДМЧС. В частности, при фиксированной вероятности D и $N = 10$, $L = 5$ отношение сигнал / шум (помеха) на входе ФС уменьшается в 2,23 раза для ПДМЧС и в 5 раз для ДСЧЧМ по сравнению с ДМЧС.

Заключение

В данной работе рассмотрена задача повышения эффективности обнаружения беспилотных летательных аппаратов (БПЛА) с использованием дискретно-модулированных по частоте сигналов (ДМЧС) и их системных

вариантов (СДМЧС), включая последовательности ДМЧС (ПДМЧС) и дискретные составные частотные сигналы с частотной манипуляцией (ДСЧЧМ).

Разработана математическая модель устройства обнаружения, реализованного на основе многоканального управляемого фильтра сжатия, и выполнено моделирование его работы на ЭВМ. Проведён сравнительный анализ вероятностей правильного обнаружения для различных сигналов при наличии шумов и помех. Полученные результаты подтвердили, что:

- Увеличение размерности ДМЧС приводит к значительному улучшению характеристик обнаружения и снижению уровня боковых лепестков в теле функции неопределенности;
- Использование ПДМЧС и ДСЧЧМ обеспечивает дополнительное повышение вероятности обнаружения по сравнению с одиночным ДМЧС;
- При заданной вероятности ложной тревоги использование СДМЧС позволяет уменьшить требуемое отношение сигнал/шум на входе фильтра в 2–5 раз.

Таким образом, предложенные сигналы и архитектура обработки обеспечивают надёжное обнаружение БПЛА, улучшая помехоустойчивость, скрытность и дальность действия радиолокационной системы.

Литература

1. В. В. Ахияров, С. И. Нефедов, А. И. Николаев и др. Радиолокационные системы. Изд. МГТУ им. Н. Э. Баумана, 2018.
2. Гаврилов К.Ю., Каменский И.В., Кирдяшкин В.В., Линников О.Н. Моделирование и обработка радиолокационных сигналов в Matlab. Издательство "Радиотехника". 2020.
3. Доклады и статьи ежегодной научно-практической конференции «Перспективы развития и применения комплексов с беспилотными летательными аппаратами», г. Коломна, 2016.
4. Плёкин В. Я., Нгуен Тхань Хынг. Формирование функции неопределенности дискретно-кодированных по частоте сигналов с заданными свойствами // Радиоэлектроника. — 2004. — № 1. — С. 3 – 11. (Изв. высш. учеб. заведений).
5. Eric Blaine Quist. UAV Navigation and Radar Odometry. Brigham Young University. 2015.
6. Nadav Levanon, Eli Mozeson. Radar Signals. Published by John Wiley & Sons. 2004.

DETECTION OF UNMANNED AERIAL VEHICLES USING FREQUENCY-DISCRETELY MODULATED SIGNALS (FDMS) AND FDMS-BASED SYSTEMS (FDMS SYSTEMS)

PhD Nguyen Thanh Hung

Le Quy Don Technical University, Vietnam Republic

This paper addresses the problem of radar detection of unmanned aerial vehicles (UAVs) using frequency-discretely modulated signals (FDMS) and corresponding systems (FDMS systems). The formation and processing characteristics of FDMS are presented, along with their advantages in detecting low-observable and maneuvering targets under strong interference conditions. It is shown that due to their high range resolution and strong interference resistance, such signals provide a high probability of UAV detection with a low false alarm rate. Numerical simulation results are presented to confirm the effectiveness of the proposed approach in comparison with traditional continuous-wave modulated signals.



МЕТОДЫ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ДАЛЬНОМЕРНЫХ ИЗМЕРЕНИЙ В РАДИОЛОКАЦИОННЫХ СИСТЕМАХ БЛИЖНЕГО ДЕЙСТВИЯ ПРИ ВОЗДЕЙСТВИИ ПОМЕХ

асп. Марков А.С.

Национальный исследовательский университет «МИЭТ»

В работе рассмотрены методы повышения достоверности дальномерных измерений в радиолокационных системах ближнего действия при воздействии помех. Приведены основные соотношения для оценки дальности при использовании линейно-частотно модулированного (ЛЧМ) сигнала. Рассмотрены факторы, снижающие достоверность измерений: аддитивные шумы, мешающие отражения, взаимные помехи и нестабильность параметров зондирующего сигнала. Проанализированы методы повышения достоверности измерений, включая выбор параметров ЛЧМ-сигнала, спектральную обработку, согласованную фильтрацию, алгоритмы CFAR (Constant False Alarm Rate), компенсацию помех и комбинированную обработку. Показано, что наиболее перспективным направлением является применение комбинированных методов обработки сигналов, обеспечивающих устойчивую оценку дальности при одновременном воздействии различных типов помех.

Радиолокационные системы ближнего действия применяются в задачах контроля расстояния, навигации, промышленного мониторинга, робототехники и автомобильных системах помощи водителю. Одной из основных измеряемых величин в таких системах является дальность до объекта. Повышение достоверности дальномерных измерений является важной задачей, поскольку ошибки определения дальности приводят к неправильной интерпретации радиолокационной обстановки.

В радиолокационных системах ближнего действия широко применяются линейно-частотно модулированные (ЛЧМ) сигналы, обеспечивающие высокое разрешение по дальности при сравнительно простой аппаратной реализации [1, 2]. ЛЧМ-сигнал в комплексной форме может быть представлен как

$$s(t) = A \cdot \exp \left(j \cdot 2\pi \cdot \left(f_0 \cdot t + \frac{\mu \cdot t^2}{2} \right) \right),$$

где A – амплитуда сигнала, f_0 – начальная частота, $\mu = B/T$ – скорость перестройки частоты, B – полоса перестройки, T – длительность зондирующего сигнала.

Для цели, расположенной на дальности R , задержка отражённого сигнала определяется выражением

$$\tau = \frac{2 \cdot R}{c},$$

где c – скорость распространения электромагнитной волны. После смещения переданного и принятого сигналов сформируется сигнал биений с частотой

$$f_6 = \mu \cdot \tau = \frac{2 \cdot \mu \cdot R}{c}.$$

Следовательно, дальность определяется выражением

$$R = \frac{c \cdot f_6}{2 \cdot \mu}.$$

Разрешающая способность по дальности для ЛЧМ-сигнала определяется полосой частот:

$$\Delta R = \frac{c}{2 \cdot B}.$$

Из приведённых выражений следует, что точность дальномерных измерений определяется точностью оценки частоты биений, стабильностью параметров ЛЧМ-сигнала и уровнем помеховой обстановки.

К основным факторам, снижающим достоверность дальномерных измерений, относятся аддитивные шумы, мешающие отражения, взаимные помехи и нестабильность параметров ЛЧМ-сигнала [3–5]. Аддитивные шумы приводят к искажению спектра разностного сигнала и снижению точности определения частоты биений [5]. Мешающие отражения формируют дополнительные спектральные компоненты и могут приводить к появлению ложных отметок дальности. Взаимные помехи возникают при одновременной работе нескольких радиолокационных систем в близких частотных диапазонах [3, 4].

Методы повышения достоверности дальномерных измерений можно разделить на несколько групп: выбор параметров зондирующего сигнала, спектральная обработка, согласованная фильтрация, адаптивное обнаружение, компенсация помех и комбинированная обработка.

Рациональный выбор параметров ЛЧМ-сигнала позволяет повысить разрешающую способность и снизить вероятность взаимного влияния радиолокационных систем. Из выражения $\Delta R = c/(2 \cdot B)$ следует, что увеличение полосы перестройки повышает разрешение по дальности. Однако при этом возрастают требования к стабильности генератора и линейности перестройки частоты.

Спектральная обработка сигнала биений является распространённым способом оценки дальности в ЛЧМ-системах [2]. Метод прост в реализации, но чувствителен к шумам, боковым лепесткам и ложным максимумам в спектре.

Согласованная фильтрация основана на корреляционной обработке принимаемого сигнала с опорным ЛЧМ-сигналом [2]. Выходной сигнал согласованного фильтра может быть представлен в виде

$$y(\tau) = \int x(t) \cdot s^*(t - \tau) dt,$$

где $s^*(t - \tau)$ – комплексно-сопряжённый опорный сигнал. Метод обеспечивает накопление энергии полезного сигнала и повышение отношения сигнал/шум, однако требует значительных вычислительных ресурсов и чувствителен к искажениям параметров принимаемого сигнала.

Для повышения достоверности обнаружения применяются алгоритмы CFAR (Constant False Alarm Rate – алгоритмы с постоянным уровнем ложной тревоги), обеспечивающие адаптивное изменение порога обнаружения в зависимости от уровня помех [3]. В общем виде условие обнаружения может быть записано как

$$Z > T_{\text{п}},$$

где Z – значение проверяемого отсчёта или спектральной ячейки, $T_{\text{п}}$ – адаптивный порог обнаружения. Применение CFAR снижает вероятность ложного обнаружения, однако при интенсивных помехах возможен пропуск полезного сигнала.

Методы компенсации помех направлены на обнаружение и подавление мешающих компонент в принимаемом сигнале. Для взаимных помех применяются методы частотно-временной фильтрации, удаления искажённых участков сигнала и реконструкции полезной компоненты [4].

Наиболее перспективным направлением является комбинированная обработка, объединяющая спектральные, корреляционные и адаптивные методы. Такой подход позволяет повысить устойчивость измерений, однако усложняет структуру обработки.

Сравнительные характеристики основных методов повышения достоверности дальномерных измерений приведены в таблице 1

Таблица 1

Методы повышения достоверности дальномерных измерений

Метод	Преимущества	Ограничения
Оптимизация параметров ЛЧМ-сигнала	Повышение разрешающей способности; снижение вероятности взаимных помех	Повышение требований к аппаратуре и стабильности сигнала
Спектральная обработка	Простота реализации; высокая скорость обработки	Чувствительность к шумам, боковым лепесткам и ложным максимумам
Согласованная фильтрация	Повышение отношения сигнал/шум; высокая точность оценки задержки	Высокая вычислительная сложность; чувствительность к искажениям сигнала
Алгоритмы CFAR	Адаптация порога обнаружения; снижение вероятности ложного обнаружения	Снижение эффективности при интенсивных помехах и мешающих отражениях
Компенсация помех	Подавление мешающих компонент; повышение достоверности измерений	Требует оценки параметров помехи
Комбинированная обработка	Высокая устойчивость к различным типам помех	Сложность реализации и настройки

Из таблицы 1 видно, что отдельные методы повышают достоверность измерений только при определённых типах помех. Спектральная обработка эффективна при простых условиях наблюдения, согласованная фильтрация обеспечивает выигрыш по отношению сигнал/шум, а алгоритмы CFAR позволяют адаптировать порог обнаружения к изменению помеховой обстановки. При одновременном воздействии шумов, мешающих отражений и взаимных помех требуется комплексное применение нескольких методов обработки.

В работе рассмотрены методы повышения достоверности дальномерных измерений в радиолокационных системах ближнего действия при воздействии помех. Показано, что точность оценки дальности в ЛЧМ-системах определяется точностью оценки частоты биений, стабильностью параметров зондирующего сигнала и уровнем помеховой обстановки.

Наиболее перспективным направлением является разработка комбинированных методов обработки сигналов, обеспечивающих устойчивую оценку дальности при одновременном воздействии шумов, мешающих отражений и взаимных помех.

Литература

1. Атаянц Б. А., Езерский В. В., Паршин В. С. Измерение расстояния в системах ближней частотной радиолокации. М.: КУРС, 2023. 256 с.
2. Patole S., Torlak M., Wang D., Ali M. Automotive radars: A review of signal processing techniques // IEEE Signal Processing Magazine. 2017. Vol. 34. No. 2. P. 22–35. DOI: 10.1109/MSP.2016.2628914.
3. Alland S., Stark W., Ali M., Hegde M. Interference in automotive radar systems: Characteristics, mitigation techniques, and current and future research // IEEE Signal Processing Magazine. 2019. Vol. 36. No. 5. P. 45–59. DOI: 10.1109/MSP.2019.2908214.
4. Zhou W., Hao X., Yang J., Duan L., Yang Q., Wang J. Interference mitigation method for millimeter-wave frequency-modulation continuous-wave radar based on outlier detection and variational modal decomposition // Remote Sensing. 2023. Vol. 15. No. 14. Art. 3654. DOI: 10.3390/rs15143654.
5. Pirkani A., Norouzian F., Hoare E., Cherniakov M., Gashinova M. Automotive interference statistics and their effect on radar detector // IET Radar, Sonar & Navigation. 2022. Vol. 16. No. 1. P. 9–21. DOI: 10.1049/rsn2.12132.

METHODS FOR IMPROVING THE RELIABILITY OF RANGE MEASUREMENTS IN SHORT-RANGE RADAR SYSTEMS UNDER INTERFERENCE CONDITIONS

asp. Markov A.S.

National Research University «MIET»

The paper considers methods for improving the reliability of range measurements in short-range radar systems under interference conditions. The basic relationships for range estimation using a linear frequency-modulated (LFM) signal are presented. The factors reducing measurement reliability are considered, including additive noise, interfering reflections, mutual interference, and instability of probing signal parameters. Methods for improving measurement reliability are analyzed, including the selection of LFM signal parameters, spectral processing, matched filtering, CFAR (Constant False Alarm Rate) algorithms, interference compensation, and combined processing. It is shown that the most promising approach is the use of combined signal processing methods that ensure stable range estimation under the simultaneous influence of different types of interference.



О ПОСТРОЕНИИ РАДИОТЕХНИЧЕСКОЙ СИСТЕМЫ ОТНОСИТЕЛЬНОЙ НАВИГАЦИИ

проф. Орлов В.К., доц. Маругин А. С.

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

Современные требования авиационной безопасности, как правило, предполагают полеты одиночных самолетов. Навигационное обеспечение таких полетов и управление воздушным движением (УВД) реализуется на основе комплекса наземных и бортовых средств, имеющихся в распоряжении авиации.

Однако, наряду с одиночными полетами, в целом ряде видов авиации, таких как спортивная, полярная, транспортная и другие, могут применяться и групповые полеты. Управление групповым полетом, поддержание строя, совместное маневрирование представляют собой как для экипажа, так и для наземных служб УВД задачи более сложные, чем управление полетом одиночного самолета. Для управления групповым полетом необходимо соответствующее навигационное обеспечение.

Процесс решения всего комплекса задач, возникающих при управлении групповым полетом, называют межсамолетной навигацией (МСН).

Ниже рассматриваются основные принципы построения систем МСН, обеспечивающие возможность обеспечения безопасности полетов, формулируются основные требования к системе относительной навигации, являющейся основным датчиком системы МСН, определяются основные пути решения поставленных задач.

Ключевые слова: летательный аппарат, межсамолетная навигация, управление относительной навигации, система определения взаимных координат, множественный доступ с временным разделением.

В настоящее время практически все типы летательных аппаратов (ЛА) оборудуются различной аппаратурой, обеспечивающей определение на борту ЛА его положения и параметров движения в той или иной системе координат. Это, в первую очередь, приемоизмерители спутниковых радионавигационных систем (СРНС), бортовая аппаратура радиотехнических систем дальней (РСДН) и ближней (РСБН) навигации, а также автономные системы навигации (инерциальные, доплеровские и т. д.), входящие в состав пилотажно-навигационного комплекса.

Эти системы достаточно успешно решают задачи навигационного обеспечения одиночных полетов авиации и управления воздушным движением (УВД). Однако с развитием авиации становится все более очевидным, что все эти системы не в состоянии решить некоторые актуальные задачи.

Наряду с одиночными полетами, в целом ряде видов авиации, таких как спортивная, полярная, транспортная и другие, могут применяться и групповые полеты. Управление групповым полетом, поддержание строя, совместное маневрирование представляют собой как для экипажа, так и для наземных служб УВД задачи более сложные, чем управление полетом одиночного самолета. Для управления групповым полетом необходимо соответствующее навигационное обеспечение.

Процесс решения всего комплекса задач, возникающих при управлении групповым полетом, называют межсамолетной навигацией (МСН) [1].

Согласно другому источнику, межсамолетная навигация – комплекс действий экипажа и расчетов пунктов управления полетами, направленных на изменение или сохранение взаимного положения самолетов (групп) в воздушном пространстве [2].

Системой межсамолетной навигации называют совокупность бортовых радиоэлектронных средств и элементов самолетного оборудования, включающую измерители относительного положения самолетов, штатные измерители параметров полета, устройства обработки, отображения и индикации данных и команд и предназначенную для вождения самолетов в составе групп [1].

Очевидно, что основой систем МСН является определение относительных координат.

Однако управление групповым полетом – не единственная задача, требующая определения на борту ЛА относительных координат.

Плотность и интенсивность воздушного движения во многих районах мира достигли такого уровня, что обычный полет пассажирского лайнера уже с трудом можно назвать одиночным. Например, считается, что в зоне крупного аэропорта может одновременно находиться до трехсот самолетов. В этих условиях все более острой становится проблема обеспечения безопасности полетов. И вполне понятно, что решение этой проблемы только средствами бортовых систем предупреждения столкновений (БСПС) и диспетчеров служб УВД, без участия экипажа самолетов, не является оптимальным. Решающим фактором для обеспечения безопасности полетов может быть возможность экипажу самолета видеть окружающую воздушную обстановку, то есть знать взаимные (относительные) координаты и параметры относительного движения потенциально опасных участников воздушного движения.

Таким образом, возможны две принципиально различных ситуации.

В первом случае совместный полет совершает группа, состоящая из заданного (и небольшого) числа заранее известных ЛА. Эти ЛА могли взлететь как с одного аэродрома, так и с разных аэродромов и в

дальнейшем встретиться в заданном географическом районе для выполнения общей задачи. В этой ситуации определение относительных координат необходимо для решения следующих задач:

- «встреча» и сбор группы;
- выдерживание строя при групповом полете;
- групповые действия для выполнения поставленной задачи;
- роспуск группы, в частности, перед заходом на посадку.

Обычно систему, решающую эти задачи, называют системой управления групповыми действиями (СУГД), а ее основной датчик называют радиотехнической системой определения взаимных координат (РТС ОВК) [3].

Во втором случае в одном географическом районе встречается некоторое количество ЛА, не имеющих общих целей и задач. Например, такая ситуация возможна в зоне аэродрома. Взлетающие, заходящие на посадку и пролетающие ЛА, оказавшиеся в данный момент времени в данном географическом районе, имеют одну общую задачу, определяющую характер их взаимодействия, – не создавать друг другу опасных ситуаций. При этом количество взаимодействующих ЛА определяется загруженностью аэродрома. В этой ситуации для обеспечения безопасности воздушного движения важно обеспечить экипажам самолетов возможность наблюдения воздушной обстановки. Систему, которая может решить такую задачу, можно назвать локальной радиотехнической системой относительной навигации ЛА (ЛРТС ОН) [3]. Следует отметить, что в число взаимодействующих в системе ОН абонентов могут быть включены и наземные объекты, так или иначе влияющие на безопасность полетов (например, автомобили-заправщики,двигающиеся по взлетно-посадочной полосе).

В целом группу абонентов, взаимодействующих в системе ОН, можно рассматривать как сеть со случайной быстро меняющейся топологией [4].

Для построения системы ОН необходимо решить несколько основных задач:

1. Измерение (определение) относительных координат.
2. Многостанционный доступ.
3. Синхронизация работы взаимодействующих абонентов.

С точки зрения безопасности воздушного движения основным параметром относительного положения является дальность между самолетами. Очевидно, что измерение дальности методом «запрос-ответ» между всеми взаимодействующими абонентами, вполне возможное в РТС ОВК при небольшом числе ЛА в группе [3], в системе ОН практически невозможно:

- при большом числе абонентов период обновления информации будет непозволительно большим;
- случайный и быстро меняющийся состав абонентов не позволяет организовать сколько-нибудь упорядоченный алгоритм передачи запросных и ответных сигналов.

Возможны следующие варианты измерения дальностей между взаимодействующими абонентами:

- измерение дальности методом «запрос-ответ» каждым абонентом до некоторых, наиболее важных для него взаимодействующих абонентов (например, наиболее близких и опасных с точки зрения столкновения);
- измерение дальности до всех взаимодействующих абонентов «однопутевым» (беззапрсным) методом.

Последний вариант весьма желателен, так как обеспечивает на каждом из абонентов измерение дальности до всех взаимодействующих с ним абонентов, находящихся в его зоне видимости. Однако этот вариант возможен только при обеспечении высокоточной синхронизации работы абонентов и наличии в составе аппаратуры достаточно высокостабильных генераторов, обеспечивающих поддержание синхронизма [3].

Для определения относительного местоположения абонентов, кроме дальностей, необходимо определить углы – относительный пеленг и угол места. Непосредственное измерение относительных угловых координат на борту ЛА трудно выполнимо из-за сложности размещения антенн и формирования необходимых диаграмм направленности. Более целесообразным представляется определение относительных координат на основе обмена навигационной информацией.

На борту ЛА практически всегда известны собственные абсолютные координаты и вектор скорости. Канал информационного обмена дает возможность на борту каждого объекта знать абсолютные координаты и вектор скорости всех взаимодействующих объектов. Это позволяет на борту каждого ЛА определить относительные координаты всех взаимодействующих с ним ЛА в абсолютной системе координат. Расчетным путем при этом могут быть получены относительные дальности, пеленги и углы места взаимодействующих объектов [3, 5]:

$$\begin{cases} D = \sqrt{\Delta x^2 + \Delta y^2 + \Delta h^2}, \\ \alpha = \arctg \frac{\Delta y}{\Delta x} + \pi \cdot \text{rect}(\Delta x) \cdot \text{sign}(\Delta y), \\ \beta = \arcsin \frac{\Delta h}{\sqrt{\Delta x^2 + \Delta y^2 + \Delta h^2}}, \end{cases} \quad (1)$$

где Δx , Δy – относительные координаты в горизонтальной плоскости; Δh – относительная высота;

$$\text{rect}(x) = \begin{cases} 1, & \text{если } x \geq 0, \\ 0, & \text{если } x < 0, \end{cases} \quad \text{sign}(x) = \begin{cases} 1, & \text{если } x \geq 0, \\ -1, & \text{если } x < 0. \end{cases}$$

Канал информационного обмена является обязательным в системе ОН (как и в РТС ОВК) [4]. Он может быть организован, например, в диапазоне частот РСБН.

Как видно из (1), обмен информацией об абсолютных координатах позволяет определить и дальности между абонентами. Однако это не исключает актуальности и непосредственных измерений дальности для повышения надежности определения относительных координат.

Как уже отмечалось, в системе ОН может одновременно взаимодействовать большое число абонентов. Это предопределяет важность решения задачи множественного доступа.

Среди всех известных методов многостанционного доступа наиболее подходящим для системы ОН является множественный доступ с временным разделением (МДВР) [6, 7]. При этом методе некоторый (возможно, условный) цикл работы системы разбивается на временные интервалы (слоты), выделяемые абонентам для передачи своих сигналов. Так как, в отличие от РТС ОВК, в системе ОН нет возможности заранее выделить взаимодействующим абонентам их слоты, реализация МДВР в системе ОН требует построения алгоритма динамического распределения слотов (назначения каналов) с учетом неизбежного изменения топологии сети и состава абонентов. Кроме того, как и в РТС ОВК, необходима синхронизация временных сеток абонентов.

Синхронизация работы абонентов может обеспечиваться с использованием нескольких уровней. Наивысший уровень может осуществляться на основе секундных меток, формируемых приемоизмерителями СРНС. Погрешность синхронизации при этом составит доли микросекунды [8].

Синхронизация второго уровня может осуществляться на основании данных наземных радиомаяков, синхронизируемых сигналами СРНС. Точность синхронизации при этом будет практически такой же, как и в первом случае. Однако сигналы СРНС могут по ряду причин пропадать, что должно быть предусмотрено при построении системы ОН.

При отсутствии информации о точном времени от глобальных источников синхронизации первого уровня или локальных наземных источников второго уровня синхронизация в системе ОН должна осуществляться непосредственно между абонентами системы [7, 9]. То есть должна обеспечиваться автономная синхронизация на основе обмена сигналами между взаимодействующими абонентами системы.

Таким образом, для построения системы ОН необходимо разработать:

1. Алгоритм измерения дальностей
2. Алгоритм автономной синхронизации
3. Алгоритм назначения каналов при МДВР
4. Алгоритм обмена информацией.

Литература:

1. Тарасов В. Г. Межсамолетная навигация. М.: Машиностроение, 1980.
2. Справочник летчика и штурмана. М.: Военное издательство МО СССР, 1974.
3. Орлов В. К., Чернявский А. Г., Герчиков А. Г. Локальные радиотехнические системы межсамолетной навигации: Изд-во СПбГЭТУ «ЛЭТИ», 2011. 132 с.
4. Принципы построения локально-глобальной многоабонентной системы относительной навигации //А. Г. Герчиков, Г. Н. Громов, В. К. Орлов и др. Вопросы радиоэлектроники. Сер. ОВР. Вып. 21, 1990. С. 3-12.

5. Определение относительных координат в локальной радиотехнической системе с обменом данными. // В. И. Бабуров, А. Г. Герчиков, В. В. Добырин, В.К.Орлов и др. Вопросы радиоэлектроники. Сер. РЛТ. Вып. 2, 2009. С. 175-182.
6. Многостанционный доступ в локальной радиотехнической системе информационного обмена и наблюдения // В.И. Бабуров, А.Г. Герчиков, В.К.Орлов. Транспорт: наука, техника, управление. 2002, № 2. С. 33-37.
7. Синхронизация и многостанционный доступ в локальных радиотехнических системах относительной навигации / В. К. Орлов, Н. Е. Липаков, В. С. Рамаданов, Е. Г. Шанин. Изд-во СПбГЭТУ «ЛЭТИ», 2016. 129 с.
8. ГЛОНАСС. Принципы построения и функционирования / Под ред А.И. Перова и В.Н. Харисова. Изд. 4-е перераб. и доп. – М., Радиотехника. 2010. 800 с. О синхронизации в радиотехнических системах информационного обмена и наблюдения //
9. В. И. Бабуров, А. Г. Герчиков, В. К.Орлов. Транспорт: наука, техника, управление. 2001, № 8.С. 23-26.

ON THE CONSTRUCTION OF A RADIO ENGINEERING SYSTEM FOR RELATIVE NAVIGATION

Prof. Orlov V. K., doc. Marugin S.A.

St. Petersburg State Electrotechnical University "LETI"

Modern aviation safety requirements, as a rule, involve flights of single aircraft. Navigation support for such flights and air traffic control (ATC) is implemented on the basis of a set of ground and airborne facilities available to aviation.

However, along with solo flights, group flights can also be used in a number of types of aviation, such as sports, polar, transport and others. Group flight control, formation maintenance, and joint maneuvering are more complex tasks for both the crew and ground-based ATC services than flight control of a single aircraft. Appropriate navigation support is needed to control the group flight.

The process of solving the entire complex of tasks that arise when controlling a group flight is called inter-aircraft navigation.

The following are the basic principles of building MSN systems that ensure flight safety, the basic requirements for the relative navigation system, which is the main sensor of the MSN system, are formulated, and the main ways to solve the tasks set are determined.

Keywords: aircraft, inter-aircraft navigation, air traffic control, system for determining mutual coordinates, time division multiple access.



ЭМПИРИЧЕСКАЯ ОЦЕНКА ПРОХОЖДЕНИЯ КОРОТКОВОЛНОВЫХ СИГНАЛОВ ПО МНОГОСКАЧКОВОЙ ТРАССЕ МОСКВА – ВЛАДИВОСТОК

инж. Ташев Н.С.

АО «Омский научно-исследовательский институт приборостроения»

Представлен график зависимости уровня сигнала от частоты. Проведен анализ полученных результатов. Приведено описание расхождения расчётов с практическим результатом. Предложены рекомендации, направленные на повышения эффективности работы совмещённых узлов КВ радиосвязи.

Введение

Наличие связи между удалёнными корреспондентами на многоскачковых трассах определяется не только состоянием ионосферы, зависящим от солнечной активности, но и, как было выявлено в ходе настоящего исследования, техническим состоянием антенно-фидерных устройств (АФУ). В настоящей статье рассматриваются результаты зондирования 1 октября 2024 года 10 часов по московскому времени на трассе Москва – Владивосток. Передача велась на радиопередающее устройство (РПДУ) [1] мощностью 5 кВт на направленную антенну типа РГД (ромбическая горизонтальная двойная). Прием осуществлялся на совмещённом узле связи на шестиметровые антенны типа широкополосный вертикальный излучатель (ШВИ) расположенные в 20 метрах друг от друга. На рисунке 1 представлены результаты приема частотно-временного сигнала (ЧВС) на I ШВИ антенну в 10:22. На рисунке 2 представлены результаты приема ЧВС на II ШВИ антенну в 10:25. Результатами приема являются зависимости уровни принятого сигнала, шума и их отношения от частоты

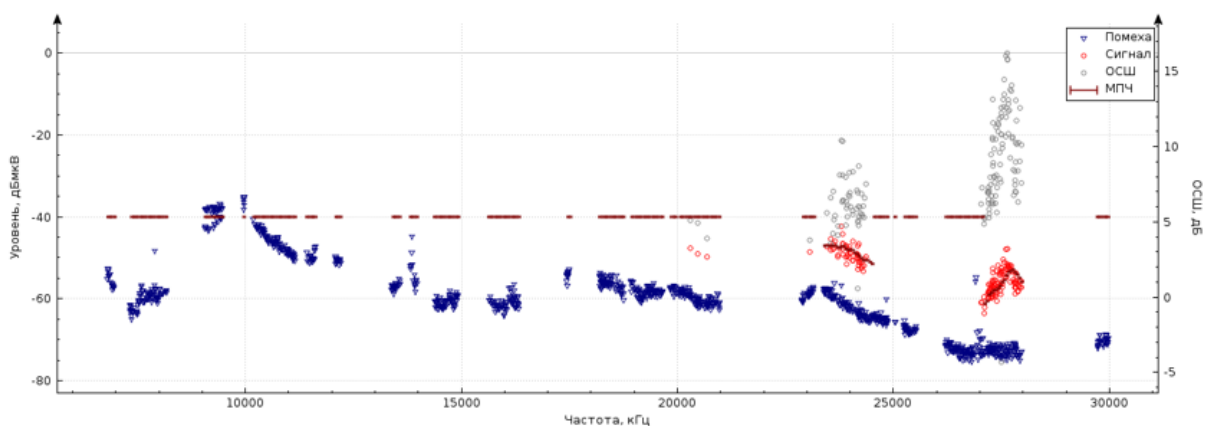


Рис. 1. График приема I антенны типа ШВИ в 10:22

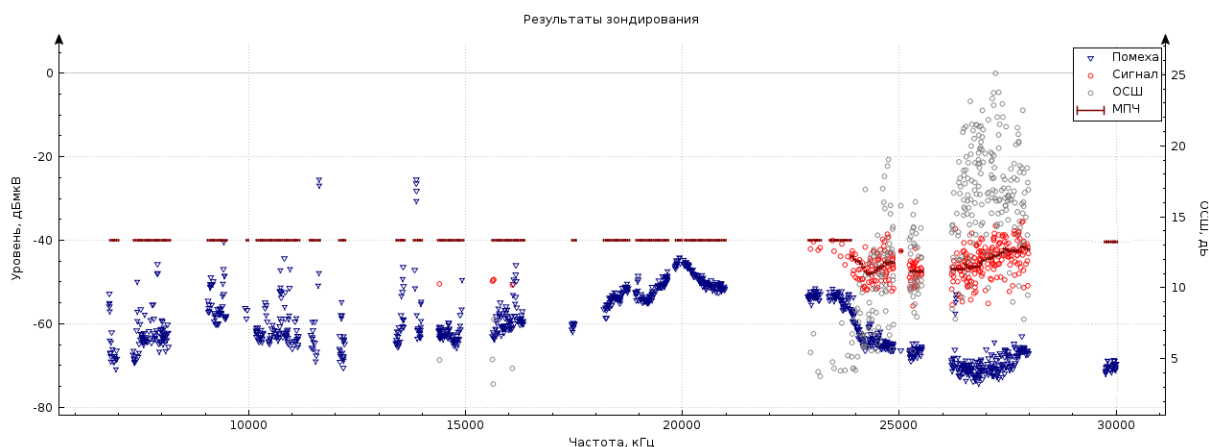


Рис. 2. График приема II антенны типа ШВИ в 10:25

Анализ экспериментальных данных

График приема I антенны типа ШВИ (рисунок 1) позволяет установить диапазон рабочих частот в данный момент времени с использованием конкретных антенн. Частотная характеристика канала является нелинейной: полезный сигнал зафиксирован в следующих диапазонах:

- 20–21 МГц: отношение сигнал/шум (ОСШ) на уровне 5 дБ;
- 23–24 МГц: ОСШ в среднем 6–7 дБ, пиковые значения до 10 дБ;
- 27–28 МГц: ОСШ в среднем 9–10 дБ, пиковые значения до 16 дБ.

График приема II антенны типа ШВИ (рисунок 2) позволяет установить диапазон рабочих частот в данный момент времени с использованием конкретных антенн. Частотная характеристика канала является нелинейной: полезный сигнал зафиксирован в следующих диапазонах:

- 14–16 МГц: отношение сигнал/шум (ОСШ) на уровне 5 дБ;
- 23–26 МГц: ОСШ в среднем 10–15 дБ, пиковые значения до 19 дБ;
- 26–28 МГц: ОСШ в среднем 17–18 дБ, пиковые значения до 25 дБ.

Сравнение с расчётными данными

На этапе предварительных расчётов при среднем недельном числе солнечных пятен $W = 150 \pm 50$ [2] были получены следующие значения: максимальная применимая частота – 22,3 МГц, оптимальная рабочая частота – 18,9 МГц, нижняя применимая частота – 15,1 МГц.

Сопоставление экспериментальных результатов с расчётными показывает, что фактические значения МПЧ (28 МГц) превышают расчётные. Известно, что с ростом частоты ослабление сигнала за счёт поглощения в ионосфере уменьшается [3]. Следовательно, в исходной расчётной модели, вероятно, была допущена ошибка, приведшая к занижению МПЧ. Полное отсутствие сигнала приема на I антенну типа ШВИ в диапазоне 25–27 МГц объясняется, по-видимому, медленными замираниями [4] или рассогласованием антенно-фидерных устройств.

Практические рекомендации по повышению эффективности совмещенных узлов КВ радиосвязи

Для увеличения суточного времени устойчивой связи было принято решение накапливать месячную статистику сеансов связи и сформировать алгоритм повышения эффективности работы совмещённых узлов радиосвязи (СУРС). При модернизации СУРС разработан следующий алгоритм:

1. Рекомендуется проводить регулярный контроль коэффициента стоячей волны и использовать согласующие устройства. Для уменьшения влияния рассогласованных передающих (ПдАФУ) антенно-фидерных устройств.
2. Синтез (сопоставление) данных ионосферно-волновой частотно-диспетчерской службы (ИВ ЧДС) с характеристиками ПдАФУ и ПрАФУ. При выборе рабочих частот следует учитывать частотную зависимость КСВН антенных систем.
3. При выборе приёмных устройств (ПрУ) обращать внимание на требования по блокированию (устойчивости к перегрузке), а также выносить ПдАФУ на достаточное расстояние для обеспечения качественных услуг связи с учётом удалённости корреспондентов.

Заключение

Экспериментальные сеансы связи не подтвердили соответствие данных, полученных на этапе расчётов, поскольку при проведении расчётов не были учтены фактическое состояние АФУ и высокочастотного тракта, а также помеховая обстановка в точке размещения ПрАФУ. Накопление месячной статистики позволило получить представление о временной структуре прохождения сигнала в течение суток и скорректировать прогноз установления связи.

Литература

1. Дудин А. Ю., Захаревич В. В., Романов Ю. В., Сорокин В. В. Использование КВ-радиопередающих устройств разработки АО «ОНИИП» для зондирования ионосферы // Техника радиосвязи. 2023. Выпуск 4 (59). С. 9–16.

2. Страница сайта «Федеральное государственное бюджетное учреждение науки Институт Земного магнетизма, ионосферы и распространения радиоволн им. Н.В. Пушкова Российской Академии наук» [Электронный ресурс]. – Режим доступа:
<https://www.izmiran.ru/services/saf/archive/ru/2024/obzor20240930.ru>
3. Дымович И. Д. Ионосфера и её исследование. М. : Энергия, 1964. 42 с.
4. Кеннеди Р. Каналы связи с замираниями и рассеянием: пер. с англ. / под ред. И. А. Овсеевича. М. : Сов. радио, 1973. 304 с.

EMPIRICAL ASSESSMENT OF THE PROPAGATION OF HIGH-FREQUENCY SIGNALS ALONG THE MULTI-HOP MOSCOW – VLADIVOSTOK ROUTE

engineer, Tashev N.S.

Omsk Scientific Research of Instrument Engineering

A graph showing the dependence of signal level on frequency is presented. An analysis of the obtained results is carried out. A description of the discrepancy between the calculated and experimental results is provided. Recommendations aimed at improving the efficiency of combined HF radio communication centers are proposed.



ОЦЕНКА ВЛИЯНИЯ ВЕТРА НА СЕЧЕНИЕ ОБРАТНОГО РАССЕИВАНИЯ ПОВЕРХНОСТИ ВНУТРИКОНТИНЕНТАЛЬНЫХ ВОДОЁМОВ

к.ф.-м.н., Ященко А.С.^{1,2},
к.т.н. Шагарова Л.В.¹,
к.ф.-м.н., Кривальцевич С.В.^{1,2},

1 Институт радиофизики и физической электроники (Омский научный центр СО РАН)
2. Омский НИИ приборостроения (АО ОНИИП)

Представлены результаты анализа данных, полученных спутниковым радиолокатором Sentinel-1B для территории юга Омской области. Обнаружена корреляционная связь между значениями удельной эффективной площади рассеивания на вертикальной поляризации, соответствующими одному из внутриконтинентальных водоёмов Западной Сибири, и скоростью приводного ветра. Полученные результаты могут найти применение как при решении задач тематического картирования по данным радиолокаторов, так и определении радиофизических характеристик подстилающей поверхности, в частности, коэффициента отражения в дециметровом диапазоне волн.

Актуальность

Системы дистанционного зондирования Земли (ДЗЗ) позволяют получать значительные объёмы информации о текущем состоянии поверхности нашей планеты, которую при описании систем радиосвязи принято считать «подстилающей поверхностью», во многом определяющей параметры излучающих систем и поглощения радиоволн при их распространении поверхностной волной, а также потери энергии при отражении радиоволн от земли и воды при распространении волной пространственной (ионосферной). Последнее относится к системам дальней (на расстояния в несколько тысяч км) радиосвязи коротковолнового (КВ или дециметрового) диапазона.

Современное развитие средств вычислительной техники и телекоммуникационных систем позволяет одновременно решать прогностические задачи по определению участков поверхности Земли, оказывающих влияние на излучение и распространение радиоволн и задачи оперативного сбора информации о текущем состоянии поверхности на данном участке (наличии/отсутствии снега, льда, влажности почвы, растительности и др.). Совместное применение данной информации при решении задач прогнозирования условий распространения радиоволн на различных радионаправлениях КВ радиосвязи и интеллектуального управления связью представляется актуальным и заслуживающим детального рассмотрения.

Существующие «геометрооптические» модели многоскачкового распространения радиоволн КВ диапазона описывают поочерёдное отражение волны от ионосферы и поверхности Земли [1-2]. При этом при моделировании часто используются значения потерь при однократном отражении от Земли в диапазоне 0÷2 дБ. Это приближение вполне оправдано, так как при отражении от ионосферы, в зависимости от её состояния, наблюдаются значительно большие потери энергии радиоволны порядка 10÷100 дБ. При рассмотрении многоскачковых радиотрасс дальней радиосвязи (дальностью более 3000 км) необходимость более точного учёта потерь при отражении от Земли возрастает т.к. растёт количество таких отражений. Актуальность такого учёта отмечается в работе [3], где представлен способ расчета одной из важных энергетических характеристик КВ-канала связи – потерь ВЧ-радиоволны при отражении от поверхности Земли на многоскачковых радиопутьях. Авторами подробно описан алгоритм нахождения потерь отражения, учитывающий рабочую частоту, угол падения луча, его поляризацию, а также параметры поверхности отражения. Именно эти параметры и могут быть определены по данным дистанционного зондирования Земли и применены в предлагаемых модельных описаниях работы радиосистем.

В последние десятилетия наблюдается рост числа ресурсных спутников с установленными на борту радиолокаторами с синтезированной апертурой (РСА). Данные многих из них находятся в открытом доступе, что позволяет получать информацию об интересующем участке поверхности Земли вне зависимости от времени суток и наличия облачности. Значения удельной эффективной площади рассеивания (УЭПР), измеряемой спутниковым РСА, определяется, в основном, особенностями геометрии поверхности (степенью шероховатости) зондируемых объектов, что позволяет решать задачи тематического картирования посредством анализа характеристик рассеянного сигнала. Физические основы тематического картирования

состояния поверхности по данным спутниковых радиолокаторов описаны в [4, 5]. С запуском спутников серии Sentinel-1 (в рамках программы Copernicus), с установленным на борту РСА С-диапазона, появилась возможность получать данные о сечении обратного рассеивания в глобальном масштабе с высокой периодичностью и пространственным разрешением (по сравнению со спутниками предыдущего поколения). Для УЭПР подстилающей поверхности характерна сезонная изменчивость, обусловленная, в основном, культивированием сельхозугодий, вегетацией растений и метаморфизмом снежного покрова. В зависимости от типа поверхности вариации УЭПР в течении года могут достигать нескольких десятков децибел. При этом изменения сечения обратного рассеивания могут носить как скачкообразный характер, например при вспашке полей, так и монотонный, в процессе формирования снежного покрова и увеличения зелёной массы растений. Геометрия поверхности водоёмов, в отличие от суши, существенно зависит от текущих условий окружающей среды. Проведённый обзор литературных источников показал, что между данными о УЭПР озёр, полученными спутниковыми РСА, и скоростью приводного ветра имеется корреляционная зависимость [6, 7]. Однако значение коэффициента корреляции между этими параметрами определяется площадью зеркала внутриконтинентального водоёма. В связи с этим задача пополнения базы знаний о взаимосвязи сечения обратного рассеивания, измеренного спутниковыми РСА, со скоростью приводного ветра для внутриконтинентальных водоёмов, отличающихся размерами, глубиной и местоположением является актуальной.

В работе использовались значения УЭПР озера Эбейты, измеренные РСА Sentinel-1B, а также данные о скорости ветра ERA5-Land и измеренные наземной метеостанцией за май-октябрь 2017-2021 гг. Космический аппарат Sentinel 1B запущен Европейским космическим агентством в 2015 г. На его борту установлен РСА С-диапазона (частота 5,4 ГГц). В зависимости от поставленных задач РСА производит либо в режиме полной поляризации (при высокодетальной съёмке отдельных участков поверхности), либо в режиме VV+VH (в режиме непрерывного получения данных со средним пространственным разрешением). Углы зондирования участка поверхности, включающего озеро Эбейты, составляли 31° и 41° для орбит 49 и 151 соответственно. Данные ERA5-Land представляются Европейским центром среднесрочных прогнозов погоды (ECMWF) с периодичностью один раз в час начиная с 1950 г. по настоящий момент времени. В качестве источника наземных метеоданных была выбрана наиболее близкая к озеру Эбейты станция, расположенная в посёлке Полтавка Омской области (номер 28786 в перечне Всемирной метеорологической организации). Из архива данных о скорости ветра выбирались наиболее близкие к времени получения радиолокационного снимка.

В результате проведённого статистического анализа данных была обнаружена корреляционная взаимосвязь между значениями УЭПР в режиме VV и скоростью ветра (таблица 1).

Таблица 1

Значения коэффициентов корреляции между значениями скорости ветра и УЭПР

Ряды радиолокационных данных (орбита КА)	Поляризация Sentinel-1	Ряды метеоданных	Время (время, UTC)	Корреляция Пирсона
УЭПР_orb49	VV	Скорость ветра ERA5-Land	02:00	0,79
УЭПР_orb151	VV	Скорость ветра ERA5-Land	02:00	0,71
УЭПР_orb49	VH	Скорость ветра ERA5-Land	02:00	-0,01
УЭПР_orb151	VH	Скорость ветра ERA5-Land	02:00	-0,07
УЭПР_orb49	VV	Скорость ветра, метеостанция	03:00	0,70
УЭПР_orb151	VV	Скорость ветра, метеостанция	03:00	0,70
УЭПР_orb49	VH	Скорость ветра, метеостанция	03:00	-0,03
УЭПР_orb151	VH	Скорость ветра, метеостанция	03:00	0,04

Как можно видеть из приведённых данных корреляционная зависимость между УЭПР в режиме VH и скоростью ветра отсутствует. Данный факт объясняется наличием неровностей у взволнованной поверхности водоёма в вертикальной плоскости.

Стоит отметить, что значение коэффициента корреляции между скоростью ветра ERA5 и УЭПР в режиме VV несколько выше, чем между скоростью ветра, измеренной на метеостанции и УЭПР в режиме VV. Это может быть обусловлено малой градацией значений скорости ветра, измеренной наземной метеостанцией, составляющей один метр в секунду. На рисунке 1 представлена графическая зависимость между УЭПР и значением скорости ветра ERA 5.

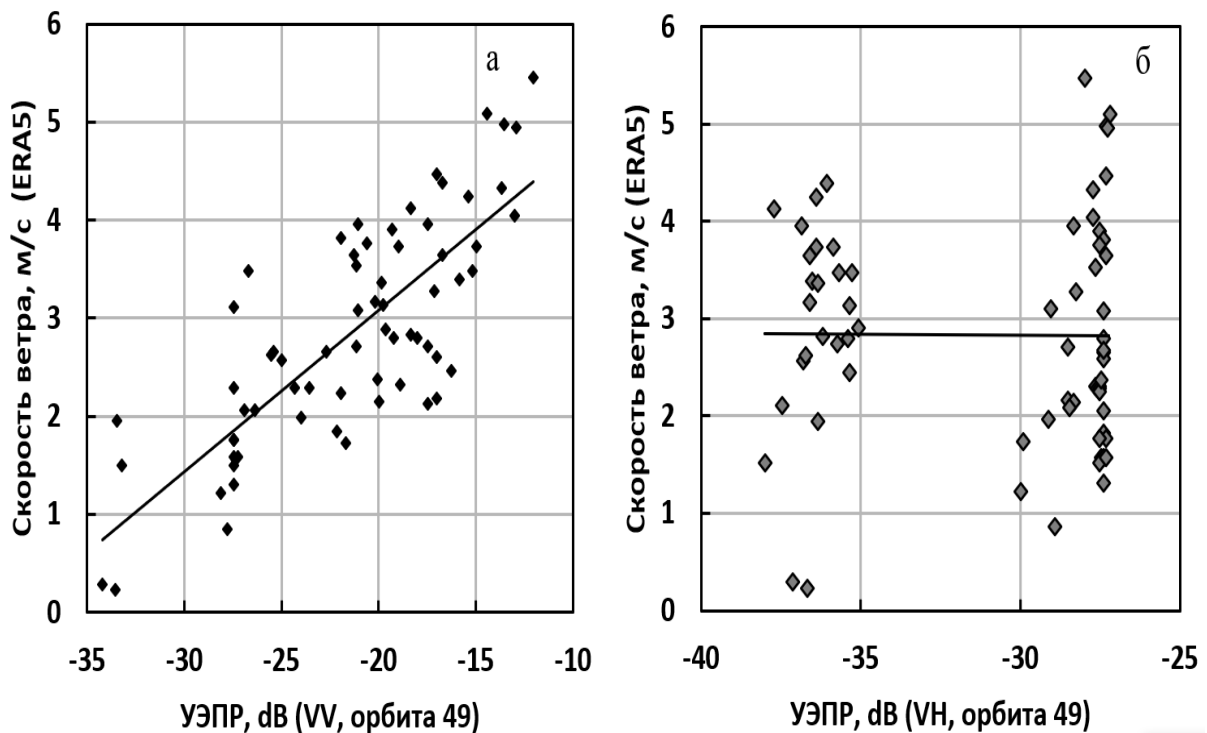


Рисунок 1 – Взаимосвязь между значениями скорости ветра ERA5 и УЭПР :
(а) – в режиме VV, (б) – в режиме VH

Таким образом проведённые исследования свидетельствуют о наличии корреляционной зависимости между скоростью ветра и УЭПР на вертикальной поляризации. Это объясняется возрастающей неровностью поверхности воды в вертикальном направлении при увеличении силы ветра. Полученные результаты могут найти применение при тематическом картировании поверхности по данным РСА, в частности при оценке неровностей поверхности и отражательных характеристик в дециметровом диапазоне волн.

Работа выполнена по государственному заданию Омского научного центра СО РАН (номер госрегистрации проекта 125013101211-4).

Литература

1. Дэвис К. Радиоволны в ионосфере. М.: «Мир». – 1973. – 504 с.
2. Романов Ю.В. О некоторых типичных ошибках построения систем высокоскоростной СВ радиосвязи // Техника радиосвязи. 2012. Выпуск 18. С. 5 -20.
3. Анишин М.М., Радио Л.П. Расчет потерь ВЧ-радиоволн при отражении от поверхности Земли // Техника радиосвязи. 2015. Выпуск № 1 (24). С. 33-41.
4. Ulaby F.T., Moore R.K., Fung A.K. Microwave Remote Sensing: Active and Passive. Vol. II: Radar Remote Sensing and Surface Scattering and Emission Theory. Boston: Artech House, 1982. 1064 p.
5. Valenzuela G.R. Theories for the interaction of electromagnetic and oceanic waves — A review // Boundary-Layer Meteorology. 1978. Vol. 13. P. 61–85.
6. Г. А. Байдаков, А. А. Кандауров, А. М. Кузнецова, Д. А. Сергеев, Ю. И. Троицкая. Натурные исследования особенностей ветрового волнения // Известия РАН. Серия Физическая. Том 82 № 11 2018. – С. 1569–1572
7. Sergeev, D., Ermakova, O., Rusakov, N., Poplavsky, E., & Gladskikh, D. Verification of C-band geophysical model function for wind speed retrieval in the open ocean and inland water conditions // Geosciences. 2023. 13(12), 361. Article 12.

ASSESSMENT OF THE IMPACT OF WIND ON THE SURFACE BACKSCATTER OF INLAND WATER BODIES

A.S. Yashchenko ^{1, 2},
L.V. Shagarova ¹, S.V.
S.V. Krivaltsevich ^{1, 2}

1. Institute of Radiophysics and Physical Electronics Omsk Science Center SB RAS
2. Omsk Scientific-Research Institute of Instrument Engineering (JSC ONIIP)

The results of an analysis of data obtained by the Sentinel-1B satellite radar for the southern Omsk region are presented. A correlation was found between the radar backscatter values for vertical polarization, and the surface wind speed corresponding to one of the inland water bodies of Western Siberia. The obtained results can be used both for thematic mapping problems using radar data and for determining the radiophysical characteristics of the underlying surface, in particular, the reflectivity in the high frequency range.



МЕТОДЫ ИЗМЕРЕНИЯ ШУМОВЫХ ХАРАКТЕРИСТИК РАДИОЧАСТОТНЫХ КОМПОНЕНТОВ ФОРМИРОВАТЕЛЕЙ СИГНАЛОВ

к.т.н. Королев А.В.

АО «Всероссийский НИИ радиотехники»

В докладе рассмотрены три метода измерения вносимых фазовых шумов устройств с отличающимися частотами входных и выходных сигналов, предназначенных для использования в формирователях сигналов радиочастотного диапазона. Показано, что использование умножителей частоты с низким уровнем собственных фазовых шумов позволяет выполнить измерение вносимых фазовых шумов при наличии одного образца исследуемого устройства в измерительном тракте аналогичном тракту измерения вносимого фазового шума усилителей с использованием анализатора фазового шума R&S FSWP. Приведены результаты измерений вносимых фазовых шумов умножителя частоты и цифровых вычислительных синтезаторов.

Прогнозирование спектральных характеристик сигналов формирователей и усилителей мощности невозможно без информации о шумовых характеристиках радиочастотных компонентов, используемых в этих устройствах. Производители элементной базы дают ограниченные сведения о фазовых шумах усилителей, смесителей, умножителей частоты, ЦАП, ЦВС и других элементов. Единственным вариантом в этом случае становится непосредственная оценка фазовых шумов, выполняемая разработчиком радиоэлектронной аппаратуры.

Метод трех преобразователей позволяет исследовать устройства с низким уровнем вносимых фазовых шумов [1]. Использование стенда, показанного на рисунке 1, позволило оценить спектральную плотность мощности фазовых шумов (СПМ ФШ) вносимых удвоителем частоты типа FK-3000+ на частотах выходного колебания 240 МГц и 2 ГГц и отстройке 1 кГц на уровне минус 162 дБн/Гц (рисунок 2). Для метода трех преобразователей необходимы три одинаковых устройства, что в ряде случаев затрудняет измерение характеристик новых элементов, имеющих в единичных экземплярах.

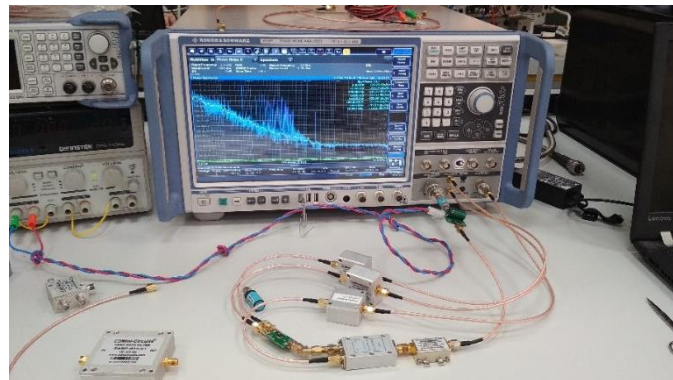


Рисунок 1. Стенд для измерения вносимых фазовых шумов умножителей частоты.

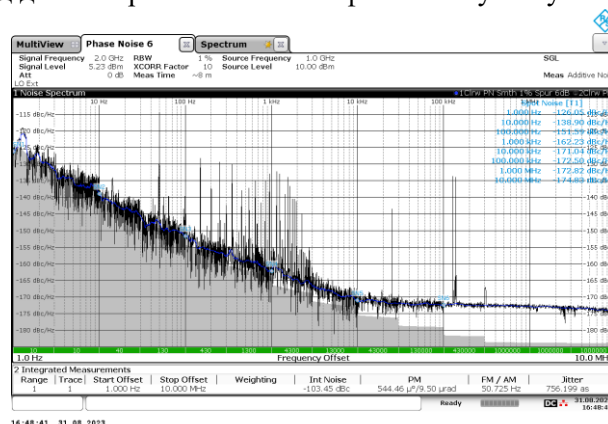


Рисунок 2. СПМ ФШ удвоителя частоты FK-3000+ на частоте выходного колебания 2 ГГц.

Достаточно низкий уровень вносимых фазовых шумов умножителей частоты и усилителей позволяет в ряде случаев провести измерение для одного образца исследуемого устройства. На рисунке 3 показан стенд для измерения вносимых фазовых шумов цифровых вычислительных синтезаторов (ЦВС), реализующий такой метод. Схема измерений приведена на рисунке 4.

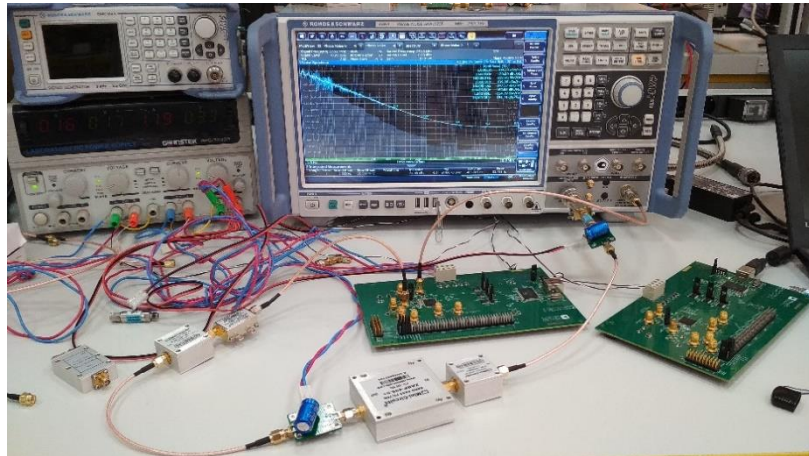


Рисунок 3. Стенд для измерения вносимых фазовых шумов ЦВС.

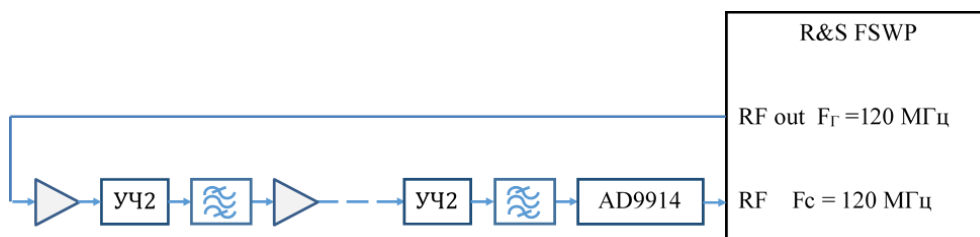


Рисунок 4. Схема измерений шумов ЦВС.

Колебание от внутреннего источника сигналов R&S FSWP с частотой f_T поступает на умножитель частоты, состоящий из последовательно соединенных удвоителей частоты УЧ2 типа FK-3000+. Макет технологического трехкаскадного умножителя частоты показан на рисунке 5. Тактовая частота ЦВС при этом равна $f_T = N_x \cdot f_T$, где $N_x = 2^n$ n - количество каскадов умножения частоты.

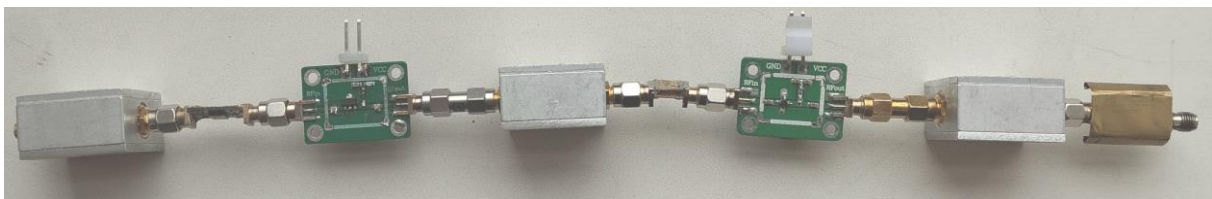


Рисунок 5. Технологический трехкаскадный умножитель частоты, $N_x = 8$.

Фликкерная и естественная составляющие фазовых шумов, вносимые многокаскадным умножителем частоты, могут быть найдены по формуле

$$S_{-1\phi N}(F) = \sum_{i=1}^n 2^{2(i-1)} \cdot (S_{-1\phi yci}(F) + S_{-1\phi yч2i}(F)),$$

$$S_{0\phi N} = \sum_{i=1}^n 2^{2(i-1)} \cdot (0,5kT_0 \cdot K_{ши}/P_{вхyci} + S_{0\phi yч2i}),$$
(1)

Здесь $S_{-1\phi yч2i}(F)$ и $S_{0\phi yч2i}$ - фликкерная и естественная составляющие СПМ ФШ вносимых удвоителем частоты УЧ2_{*i*}, $S_{-1\phi yci}(F)$ - фликкерная составляющие СПМ ФШ вносимых усилителем, $P_{вхyci}$ и $K_{ши}$ - коэффициенты усиления и шума усилителя i -го каскада. СПМ ФШ усилителей не зависит от частоты усиливаемого сигнала [2]. Полагая в соответствии с результатами измерений что СПМ ФШ УЧ2 не зависит от частоты в диапазоне 250...2000 МГц, формулу (1) для $S_{-1\phi yч2N}(F)$ и $S_{0\phi yч2N}$ можно упростить. При идентичных УЧ2 и усилителях во всех каскадах, при $n = 2 \dots 5$ можно с погрешностью, не превышающей $0,1 \cdot (n - 2)$ [дБ] можно учитывать шумы только первых двух каскадов умножения частоты.

В нашем случае измерение производится на частоте равной частоте внутреннего источника сигналов измерителя FSWP. Выходная частота ЦВС f_c связана с f_T соотношением $f_c = f_T \cdot K$. При $f_c = f_T$ коэффициент

передачи ЦВС равен $K_{\text{ЦВС}} = 1/N_x$. Тогда составляющие СПМ ФШ, вносимых умножителем частоты на выходе ЦВС равны

$$S_{-1\phi_{NK}}(F) = S_{-1\phi_N}(F) \cdot K_{\text{ЦВС}}^2, S_{0\phi_{NK}} = S_{0\phi_N} \cdot K_{\text{ЦВС}}^2. \quad (2)$$

Данный метод по структуре измерительного тракта аналогичен методу измерения вносимого фазового шума усилителей [3].

В таблице 1 приведены рассчитанные по формулам (1) и (2) значения СПМ ФШ $S_{-1\phi_N}(F)$, $S_{0\phi_N}$ на выходе умножителя на частоте f_T и $S_{-1\phi_{NK}}(F)$ и $S_{0\phi_{NK}}$ на выходе ЦВС при отстройке от несущей $F = 1$ кГц и в области естественных шумов и четырех значениях коэффициента умножения N_x .

Таблица 1

Расчетные значения СПМ ФШ

N_x	$S_{-1\phi_N}(F)$, дБн	$S_{0\phi_N}$, дБн	$S_{-1\phi_{NK}}(F)$, дБн	$S_{0\phi_{NK}}$, дБн
4	-153.37	-163.24	-165.37	-175.24
8	-147.02	-156.87	-165.02	-174.87
16	-141.00	-150.84	-165.00	-174.84
32	-134.97	-144.82	-164.97	-174.82

На рисунке 6 показана СПМ ФШ $S_{\phi_{\text{ВЫХ}}}(F)$ колебания на выходе ЦВС AD9914 измеренная при $f_c = 250$ МГц, $f_T = 1$ ГГц, $N_x = 4$ в схеме рисунка 4. Запишем $S_{\phi_{\text{ВЫХ}}}(F) = S_{-1\phi_{\text{ВЫХ}}}(F) + S_{0\phi_{\text{ВЫХ}}}$, где $S_{-1\phi_{\text{ВЫХ}}}(F) = S_{-1\phi_{\text{ЦВС}}}(F) + S_{-1\phi_{NK}}(F)$, $S_{0\phi_{\text{ВЫХ}}} = S_{0\phi_{\text{ЦВС}}} + S_{0\phi_{NK}}$, $S_{-1\phi_{\text{ЦВС}}}(F)$ и $S_{0\phi_{\text{ЦВС}}}$ – СПМ ФШ вносимых ЦВС. При измеренных значениях $S_{-1\phi_{\text{ЦВС}}}(F) = -139,36$ дБн, $S_{0\phi_{\text{ЦВС}}} = -154,66$ дБн, с учетом данных таблицы 1 погрешность измерения не превышает 0,01 дБ на частоте отстройки 1 кГц и 0,04 дБ в области естественных шумов, что значительно меньше погрешности 1,5 дБ анализатора фазового шума R&S FSWP [3].

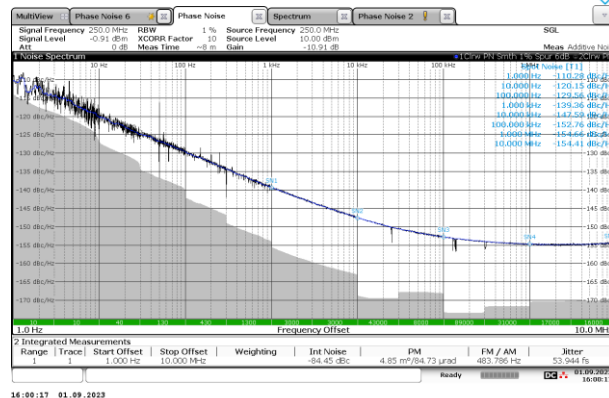


Рисунок 6. СПМ ФШ колебания на выходе ЦВС AD9914.

При необходимости выполнить измерение вносимых фазовых шумов ЦВС, работающих в высоких зонах Найквиста на образах основной частоты, можно использовать метод, приведенный в [4] и модифицированный для использования анализатора фазового шума R&S FSWP. Схема измерения приведена на рисунке 7.

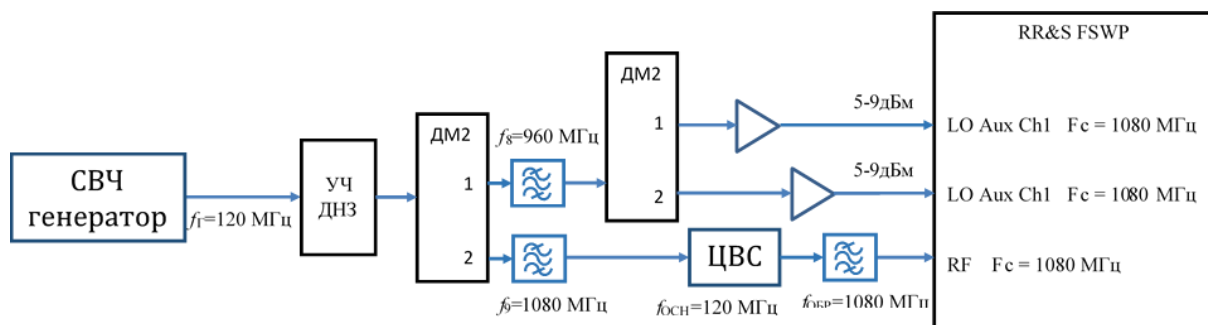


Рисунок 7. Схема измерения СПМ ФШ ЦВС на образах основной частоты.

Частота выходного колебания СВЧ генератора $f_T = 120$ МГц. В схеме используется генератор гармоник (ГГ), выполненный на диоде с накоплением заряда (ДНЗ). Макет ГГ на ДНЗ показан на рисунке 8, ГГ с делителем частоты и фильтром гармоник – на рисунке 9.

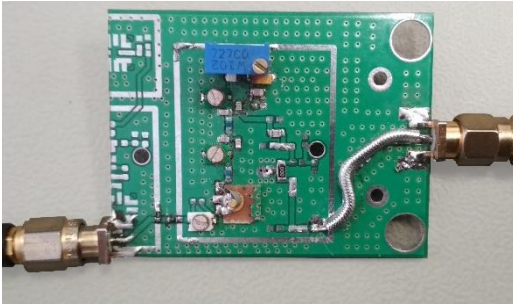


Рисунок 8. Макет генератора гармоник на ДНЗ.

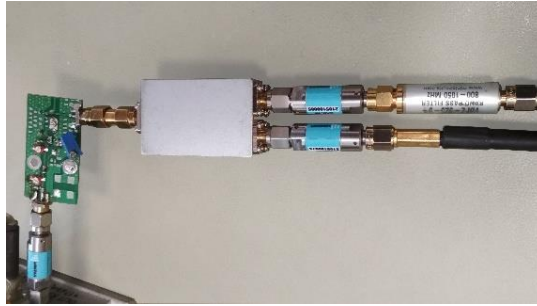


Рисунок 9. Умножитель частоты на ДНЗ с делителем мощности.

В схеме используются 8-я и 9-я гармоники выходного сигнала ДНЗ с частотами f_8 и f_9 . Вносимые фазовые шумы ДНЗ малы [5], что позволяет эффективно подавить их в схеме с двумя опорными каналами [3]. Внешний СВЧ генератор имеет достаточно высокую мощность для возбуждения ДНЗ. Фазовые шумы ДНЗ на частотах гармоник коррелированы, и для СПМ ФШ $S_{\phi_{ДНЗ}}$ на частотах гармоник с номерами i и j справедливо соотношение

$$S_{\phi_{ДНЗ}fi}/S_{\phi_{ДНЗ}fj} = (i/j)^2$$

Тактовая частота ЦВС $f_T = f_8 = 960$ МГц, коэффициент передачи ЦВС $K_{ЦВС} = 1/8$, частота образа $f_{обр} = f_8 + f_8 \cdot K_{ЦВС} = f_9 = 1080$ МГц. Измеренная СПМ ФШ ЦВС 1508ПЛ08 в третьей зоне Найквиста на частоте 1080 МГц показана на рисунке 10.

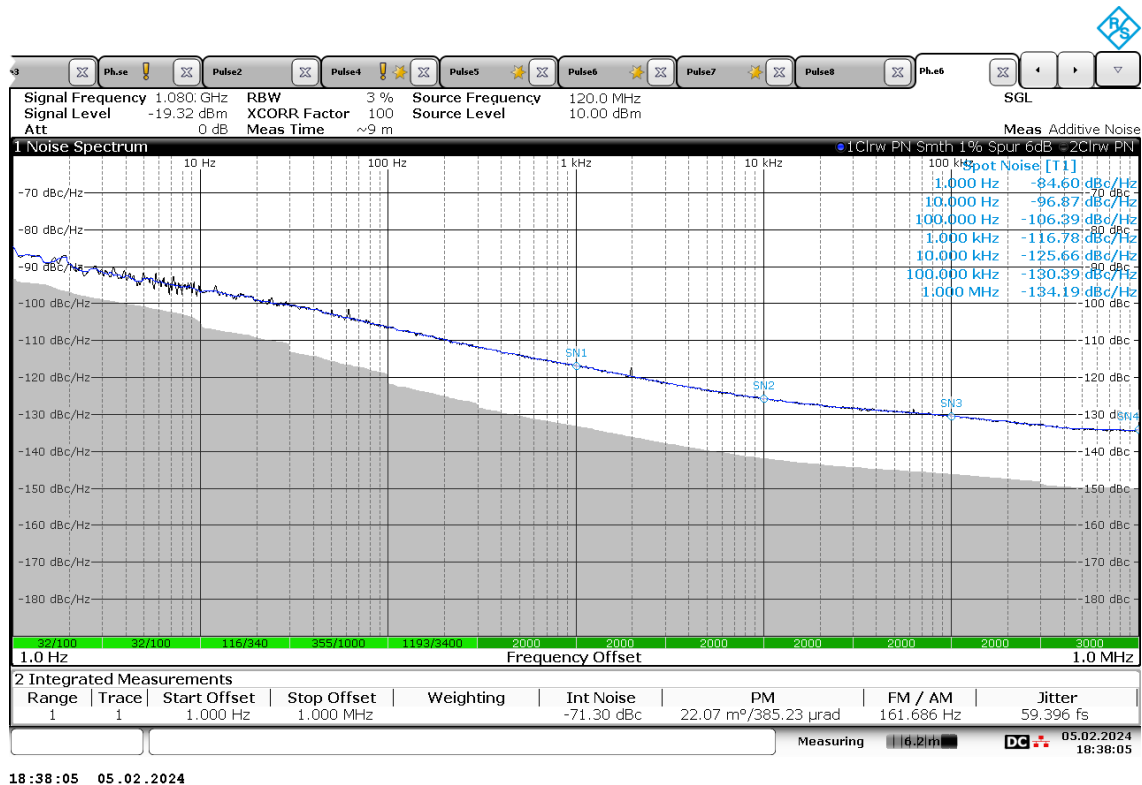


Рисунок 10. СПМ ФШ ЦВС 1508ПЛ08 в третьей зоне Найквиста на частоте 1080 МГц.

Поскольку фазовые шумы ГГ компенсируются при корреляционной обработке в анализаторе фазового шума, погрешность измерения в схеме рисунка 7 определяется только анализатором R&S FSWP и находится в пределах 1,5 дБ.

В докладе рассмотрены три метода измерения вносимых фазовых шумов элементной базы формирователей сигналов радиочастотного диапазона. Все методы ориентированы на использование анализатора фазового шума R&S FSWP. При отсутствии такого измерительного прибора, можно

использовать интерферометрический метод [5] или метод [4], позволяющие применить анализатор источников сигналов реализующий метод фазового детектора.

Литература

1. Королев А.В., Рыков С.Г. Экспериментальное исследование фазовых шумов многоканальных схем цифрового синтеза при сложении мощностей каналов цифроаналоговых преобразователей // Антенны. 2024. № 5. С. 37–46. DOI: <https://doi.org/10.18127/j03209601-202405-04>
2. Korolev A., Rykov S., Sidorov I., Gudkov A., Chizhikov S. Measuring the Phase Noise of Amplifiers for Radiometer Receivers // 2024 IEEE 9th All-Russian Microwave Conference (RMC). – IEEE, 2024. – С. 180-183.
3. Rohde & Schwarz R&S®FSWP Phase Noise Analyzer. - Текст : электронный / Specifications. Version 04.00, August 2016. 32 с. - URL: <https://www.rohdeschwarz.com/> - (дата обращения: 21.05.2021).
4. Патент № 2807958 С1 Российская Федерация, МПК G01R 29/26. Система для измерения вносимого фазового шума устройства высокочастотного, сверхвысокочастотного или оптического диапазонов : № 2023123805 : заявл. 14.09.2023 : опубл. 21.11.2023 / А. В. Королев, Я. В. Коршиков, Д. А. Костючик, С. Г. Рыков ; заявитель Акционерное общество "Всероссийский научно-исследовательский институт радиотехники". – EDN KGXSCA.
5. Измерение вносимых фазовых шумов элементов радиочастотного тракта радиометрических приемников / А. В. Королев, С. Г. Рыков, И. А. Сидоров [и др.] // Электромагнитные волны и электронные системы. – 2024. – Т. 29, № 3. – С. 88-96. – DOI 10.18127/j5604128-202403-09. – EDN UVGCEU.

METHODS FOR MEASURING THE NOISE CHARACTERISTICS OF RADIO FREQUENCY COMPONENTS OF SIGNAL GENERATORS

Cand.Tech.Sci. Korolev A.V.¹

¹ «JSC All-Russian Scientific Research Institute of Radio Engineering» (Moscow, Russia)

The report discusses three methods for measuring the additive phase noise of devices with different frequencies of input and output signals intended for use in radio frequency range signal generators. It is shown that the use of frequency multipliers with a low level of additive phase noise makes it possible to measure the additive phase noise in the presence of a single DDS sample in a measuring path similar to the measurement path of the additive phase noise of amplifiers using the R&S FSWP phase noise analyzer. The results of measurements of the additive phase noise of a frequency multiplier and direct digital synthesizers are presented.



СЕКЦИЯ № 3.

СИСТЕМЫ, СЕТИ И УСТРОЙСТВА ТЕЛЕКОММУНИКАЦИЙ, В Т.Ч. КОСМИЧЕСКИЕ, ЛАЗЕРНЫЕ, АКУСТИЧЕСКИЕ, ВОЛОКОННО-ОПТИЧЕСКИЕ И ИНЫЕ.

РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО ФОРМИРОВАНИЮ КОРПОРАТИВНОЙ СЕТИ ОРГАНИЗАЦИИ

преп. Аветисян Т.В., студ. Павлов С.Ю., студ. Дюков А.В.,
проф. Преображенский А.П., проф. Преображенский Ю.П.

Автономная некоммерческая образовательная организация высшего образования Воронежский институт высоких технологий

По мере того, как происходит развитие информационных технологий, можно наблюдать увеличение объемов данных, которые передаются в различных цифровых сетях. Важно обеспечивать поддержку гибкого управления передачи разнородного трафика. Целью исследования является разработка предложений по особенностям формирования корпоративной сети внутри организации. Показано, как осуществлять поиск маршрутов с привлечением критерия минимального времени прохождения. Основная идея состоит в том, чтобы сформировать такую модель обработки информации внутри корпоративной сети, которая бы получить наиболее оптимальные маршруты при заданных критериях.

Интеграция информационных технологий, сервисной инженерии и телекоммуникационных систем формирует новые требования к проектированию, так как современная среда характеризуется практически неограниченным числом сервисов, которые трудно поддаются традиционному описанию на основе выбранных характеристик. Существующие методы передачи информационных потоков не обеспечивают эффективную поддержку процессов предоставления композитных сервисов, где достижение цели обслуживания требует согласованного взаимодействия нескольких элементарных компонентов с существенно различающимися параметрами.

Разработчики подобных решений, учитывают вероятность ошибок, которые будут появляться на нижних уровнях эталонной модели взаимодействия открытых систем. При этом для любых условий обеспечивается возможность как можно лучшей передачи информации. Однако такая устойчивость нередко достигается ценой ухудшения качества обслуживания, что вызывает негативные и необратимые последствия для конечных пользователей [1].

Совмещение различных телекоммуникационных технологий создает основу для построения гибких и высокопроизводительных сервис-ориентированных систем, которые находят применение в разнообразных сферах. Тем не менее, процесс их широкого внедрения и дальнейшего развития сдерживается недостаточной теоретической проработанностью моделей предоставления сервисов, связанной с ограниченностью знаний о внутренней структуре сетей центров обработки данных (ЦОД).

Поэтому при организации композитного сервиса необходимо учитывать характеристики информационно-телекоммуникационной инфраструктуры, что позволяет оптимизировать выбор элементарных компонентов или реализовать их динамическую миграцию в рамках виртуализированной среды.

Цель исследования – разработка и исследование модели корпоративной сети организации, обеспечивающей оптимальное распределение сетевых ресурсов, высокую отказоустойчивость

При снижении производительности конкретного сервиса система управления осуществляет миграцию этого сервиса на другую виртуальную или физическую машину. При этом логическая топология сети остаётся неизменной, однако физические пути передачи данных изменяются. В результате этого общая задержка при передаче сервиса от пользователя к центру обработки данных и обратно определяется суммарным временем, зависящим от характеристик передачи по новым физическим каналам и времени обработки запроса на обновлённой вычислительной инфраструктуре.

$$t_{пер} = \sum_1^n t_{комут.} + \sum_1^{n-1} t_{п.к.з.} + t_{обр.} \quad (1)$$

где n - считается количеством запросов; $t_{комут.}$ - временем прохождения запроса через систему коммутации; $t_{п.к.з.}$ - временем поиска каналов, по которым будет реализовываться передача; $t_{обр.}$ - временем обработки запроса, который считается суммой времени обработки запроса сервисом, состоящим из k атомарных сервисов

$$t_{обр.} = \sum_1^k t_{a.c.} \quad (2)$$

Поскольку при изменении оптимального маршрута передачи данных происходит перераспределение сетевых потоков, это приводит к увеличению времени поиска подходящих каналов связи, по которым будет осуществляться передача $t_{п.к.з.}$. В результате возрастает суммарное время доставки данных и появляется дополнительная задержка.

Для минимизации указанных потерь предлагается выполнять поиск маршрута на основе критерия минимального времени прохождения.

Рассмотрим пример: интерфейс на выходе, через который осуществляется передача данных от физического сервера А к виртуальной машине (VM), имеет значение задержки t . Если эта задержка меньше порогового значения $T (t < T)$ [2], передача проходит в нормальном режиме. Однако из-за различных факторов (нагрузка на сервер, миграция VM, изменение маршрутов) VM с установленным программным комплексом может мигрировать на физический сервер В (рисунок 1). В этом случае изменяется физический путь передачи данных, что может вызвать увеличение суммарной задержки и необходимость перерасчета оптимального маршрута.

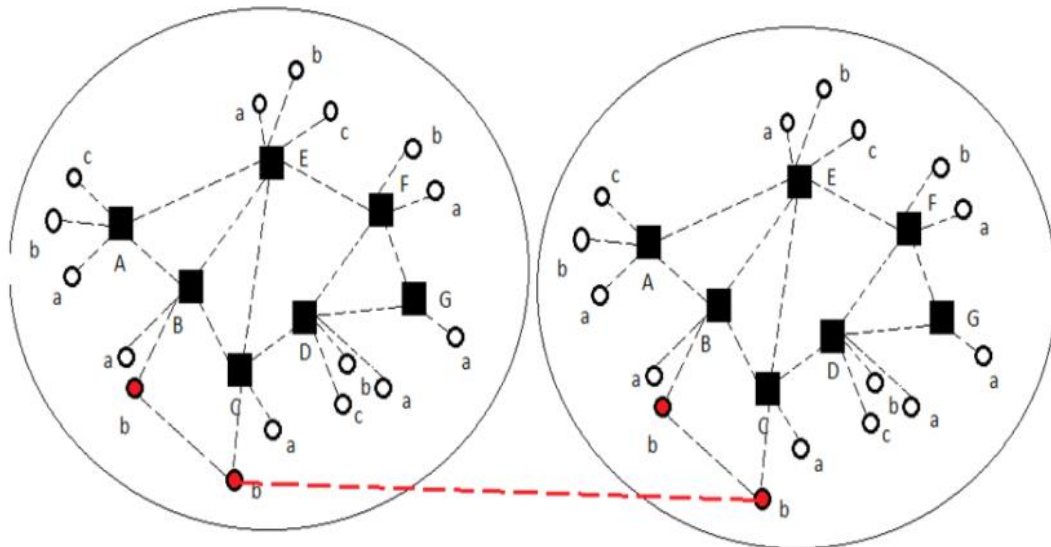


Рисунок 1 – Принцип миграции компонентов сервиса

При передаче запроса на предоставление сервиса в динамически изменяющейся структуре проводится анализ наличия логического маршрута, для которого задержка передачи каждого компонента сервиса через интерфейсы сетевых узлов t не превышает заданного порогового значения T . В случае, если из-за изменения устойчивости структуры такой маршрут отсутствует, выполняется перерасчёт комбинированной метрики с учётом актуальных значений задержки, и формируется новый маршрут для передачи запросов.

Такой подход позволяет более точно контролировать время поиска каналов передачи и поддерживать необходимый уровень QoS. Методика адаптивного расчёта маршрутов снижает время на поиск

оптимального пути, не увеличивая общий интервал передачи запросов и предотвращая их потерю, поскольку учитывается текущее состояние логической топологии сетевой платформы [3].

Для эффективного функционирования и обеспечения заданного уровня качества обслуживания информационная система должна обладать определённым запасом устойчивости к внешним дестабилизирующим воздействиям. На всю информационную систему и её отдельные компоненты могут влиять различные факторы, включая кибератаки, удаление материалов с веб-ресурсов, вывод из строя отдельных серверов, публикацию новых сервисов или компонентов, которые изменяют конфигурацию исходной системы, а также появление новых информационных систем, способных снизить актуальность или полностью заменить существующую.

В процессе анализа функциональной живучести информационной системы предполагается обеспечение поддержания необходимых связей между отдельными функциональными элементами. При оценке устойчивости в информационных сетях, таких как сети центров обработки данных, особое внимание уделяется обеспечению максимально возможной стабильности связей между компонентами сервиса. Под устойчивостью связей понимается сохранение топологических структур при передаче или миграции компонентов, то есть обеспечение наличия как физических, так и логических маршрутов при репликации компонентов.

Обозначим множество компонентов сервиса (информационных функций), предоставляемых системой ЦОД организации через $F = \bigcup_{k \in I} F_k = \{f_1, f_2, \dots, f_n\}$.

Причем каждая компонента F_k потенциально может выполнить множество функций $\varphi_n : \{1, 2, \dots, p\} \rightarrow P(F)$, где $P(F)$ - множество всех подмножеств F . Если $\varphi_n(k) = \{f_{k_1}, f_{k_2}, \dots, f_{k_j}\}, 1 \leq k_m \leq n, 1 \leq m \leq j$, то функциональная компонента F_k может выполнить функции $f_{k_1}, f_{k_2}, \dots, f_{k_j}$.

В каждый конкретный момент времени F_k выполняет определенное множество функций, определяемых $\varphi_n : \{1, 2, \dots, p\} \rightarrow P(F)$. Если $\varphi_n(k) = \{f_{k_1}, f_{k_2}, \dots, f_{k_j}\}, 1 \leq k_m \leq n, 1 \leq m \leq j$, то компонента F_k может выполнять функции $f_{k_1}, f_{k_2}, \dots, f_{k_j}$. Когда $\varphi_t(k) = \emptyset$ компонента F_k недоступна.

Каждая $f_{k_m} \in F, m = \overline{1, j}$ характеризуется эффективностью выполнения или количеством обработанных запросов на компоненте c_{k_m} . Эффективность выполнения определяется как $\varphi_{ef} : F \times \{1, 2, \dots, p\} \times P(F) \rightarrow C$, где C - некоторое числовое множество $\varphi_{ef}(f_{k_m}, k, \varphi_t(k)) = c_{k_m}$ означает, что функциональная компонента F_k выполняет функции $\varphi_t(k) = \{f_{k_1}, f_{k_2}, \dots, f_{k_j}\}$, тогда эффективность выполнения $f_{k_m} \in \{f_{k_1}, f_{k_2}, \dots, f_{k_j}\}$ равна c_{k_m} .

Тогда условие доступности предоставления компоненты (то есть эффективного обработки запросов на компоненте) будет иметь вид:

$$\begin{aligned} \bigcup_{k=1}^p \varphi_n(k) &\supseteq F \\ \varphi_t(k) &\subseteq \varphi_n(k) \forall k = \overline{1, p} \\ \sum_{k=1}^p \varphi_{ef}(f_{k_m}, k, \varphi_t(k)) &\geq c_{k_m}, \forall k_m = \overline{1, n} \end{aligned} \quad (3)$$

Если компоненты F_k функционально однородны, а цель обеспечения соответствующих параметров QoS, что обеспечивается благодаря наличию соответствующего количества доступных функциональных компонентов:

$$R(F_k, t) \geq R^* = const$$

где $R(F_k, t)$ - среднее количество доступных компонент сервиса в момент времени $t \geq 0$, R^* - минимально допустимое количество доступных компонент, при которой работоспособность системы и уровень качества обслуживания не менее определенного порогового минимума, то оценка функциональной живучести системы будет функцией:

$$N(F_k, t) = \frac{\bar{\Omega}(F_k, t)}{N_{\omega}} \quad (4)$$

где $\bar{\Omega}(F_k, t)$ - математическое ожидание работоспособности системы в момент времени $t \geq 0$; N_{ω} - суммарная доступность всех компонентов сервиса.

Фактически проблема снижения времени обработки (обслуживания) запросов, которые поступают на обслуживание в ЦОД организации, с учетом топологической структуры данного центра сводится к уменьшению средней суммарной задержки D . Однако такая задержка должна удовлетворять условиям:

$$D = \frac{1}{P_{cm}} \sum_{Deg.v} \frac{w_T(n)}{C - w_T(n)} \leq D_{зад} \quad (5)$$

Для поиска пути по критерию минимального времени прохождения максимальная задержка, при скорости 100 Мбит/с, равная 100 мс. Задержка может быть уменьшена только в том случае, когда структура центра обработки данных будет устойчивой в течение времени T . Устойчивость структуры (живучесть) предлагаем оценить на основе метода, включает в себя: оценку структуры сети (модели сети), загруженности каждой виртуальной машины в момент времени t , а также взаимосвязь узлов между собой.

Если загруженность узлов в момент времени меньше или равна максимально возможной загрузке системы, то это приведет к увеличению устойчивости структуры системы, что в свою очередь приведет к уменьшению задержки. Использование предложенного метода позволит уменьшить продолжительность поиска каналов, по которым будет осуществляться передача, поскольку уменьшится задержка, которая заложена в метрику алгоритма поиска оптимального пути, учитывающий устойчивость структуры. Это обеспечит более быструю передачу компонентов сервиса и, соответственно, ускорит его предоставление.

Вывод.

В целях повышения качества обслуживания и уменьшения времени поиска маршрута, который, бесспорно, зависит от надежности некоторых узлов, предложен метод поиска маршрута с учетом устойчивости структуры виртуализированного центра обработки данных организации. Особенностью данного метода является компромисс между выбором оптимального маршрута и требованиями к параметрам QoS.

Связано это с тем, что вероятность того, что одновременным образом реализуются потоки запросов. Которые характеризуются максимальными требованиями к качеству предоставления сервиса внутри маршрутов, проходящие через одни и те же узлы, низкая. Это дало возможность учитывать не только особенности обеспечения всевозможных показателей QoS для разнообразных классов трафика, а и политику оператора по распределению приоритетов, согласно уровню качества, заказанного абонентом.

Литература

1. Гаипов К.Э., Крикунов И.Л., Демичева А.А. Модель многокритериальной оптимизации распределения информационных потоков в телекоммуникационных сетях // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2022. № 12-2. С. 67-74.
2. Колесников К.Г., Масалкин А.А., Москвин Б.В. Параметрическая оптимизация информационного обмена в сети связи с динамически изменяющейся структурой // Труды Военно-космической академии имени А.Ф. Можайского. 2019. № 668. С. 31-36.
3. Грузликов А.М., Колесов Н.В., Литуненко Е.Г., Скородумов Ю.М. Оптимизация информационных обменов в сети автономных абонентов // Известия Российской академии наук. Теория и системы управления. 2022. Т. 6. № 6. С. 56-64.

DEVELOPMENT OF PROPOSALS FOR THE FORMATION OF THE CORPORATE NETWORK OF THE ORGANIZATION

lect. Avetisyan T.V., lect. Pavlov S.Yu., stud. Dyukov A.V.,
prof. Preobrazhensky A.P., prof. Preobrazhensky Yu.P.

Autonomic not-commercial educational organization of higher education Voronezh Institute of high
technologies (ANOO VO VIVT)

As information technology advances, it is possible to observe an increase in the amount of data that is transmitted across various digital networks. It is important to support flexible management of heterogeneous traffic. The purpose of the study is to develop proposals on the features of the formation of a corporate network within an organization. It is shown how to search for routes using the criterion of the minimum travel time. The main idea is to form such a model of information processing within the corporate network, which would get the most optimal routes under the given criteria.



РАЗРАБОТКА АЛГОРИТМА ДВУНАПРАВЛЕННОГО ПОИСКА ПУТЕЙ В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ

преп. Баскаков А.Е.

Национальный исследовательский университет «МИЭТ»

В основе концепции программно-конфигурируемых сетей лежит использование централизованного контроллера для сбора детальных сведений о топологии через протокол OpenFlow. Представление структуры связи в виде неориентированного взвешенного графа позволяет учитывать пропускную способность и задержки каждого ребра. Предложенный метод решает задачу нахождения множества пересекающихся маршрутов путем формирования вспомогательных графов. Отличительной особенностью предложенного подхода является возможность нахождения пересекающихся маршрутов, что затруднительно при использовании классических итерационных алгоритмов. Проведен теоретический анализ временной сложности, который показал, что в условиях разреженных графов предлагаемый метод позволяет снизить вычислительные затраты до 50% по сравнению с традиционными решениями. Сформулированы условия эффективности алгоритма в зависимости от параметров задержки и плотности связей топологии.

Проблема передачи больших объемов данных с установленными параметрами качества обслуживания является актуальной в настоящее время, ввиду непрерывного роста объемов передаваемого трафика, в том числе в магистральных сетях. Наличие множества децентрализованных сервисов предполагает использование различных протоколов маршрутизации, основанных на алгоритмах поиска путей. При этом большинство алгоритмов поиска путей не позволяют находить маршруты в кратчайшие промежутки времени, что подтверждает актуальность необходимости разработки новых алгоритмов и протоколов поиска путей.

В работе в качестве исходной сети связи рассматривается программно-конфигурируемая сеть (ПКС), управляемая одним контроллером. Указанный подход позволяет ввести исходные данные для разрабатываемого алгоритма – неориентированный взвешенный граф, описывающий используемую сетевую топологию. Последнее возможно ввиду использования концепции построения ПКС, а именно, управление ПКС коммутаторами с центрального устройства и обмен данными между ними с использованием протокола OpenFlow [1-2].

Так, новое устройство в сети связи отправляет к ПКС контроллеру запрос на инициализацию, а также информацию об известных соседях, скорости интерфейсов, через которые выполняется подключение к соседям, задержку передачи и т.д. Такой подход позволяет хранить на центральном устройстве актуальную информацию о подконтрольной сети и ее отдельных компонентах, а также представлять сеть в виде указанного графа, представленного как $G(V, E)$, где V – набор вершин, E – набор ребер, при этом ребра выражены через параметры b и d , пропускную способность и задержку передачи соответственно. Тогда каждое ребро может быть представлено в виде $E(b, d)$. Для вычисления метрик используем формулу $D_i = d_i + \frac{\lambda_i}{b_i}$, где λ_i – входной подпоток [3-5].

Существующие алгоритмы поиска кратчайшего пути, в большинстве случаев, предназначены для поиска одного пути на графе. Для поиска множества путей на графе алгоритмы используются в итерационном цикле, при этом найденные пути не учитываются в последующем расчете, что приводит к невозможности поиска пересекающихся путей. Таким образом, решением является разработка алгоритма поиска путей передачи данных с построением вспомогательного графа. Последний представлен через $G_d(V_d, E_d, d_i)$, а его построение может быть описано рядом действий: добавление вершин, не являющихся входной, к множеству V_d в виде значений $v^0, v^1, \dots, v^{d_i}$; добавление входной вершины к множеству V_d в виде s^0 ; ребра исходного графа, не связанные с входной вершиной добавляются к множеству E_d . Разрабатываемый алгоритм двунаправленного поиска также основан на принципе построения вспомогательного графа, но также необходимо изначальное разделение графа на подграфы. Поскольку метод разбиения графа также влияет на итоговую временную сложность, введем дополнительное ограничение, а именно, примем что исходных граф уже разбит на два подмножества. Тогда требуется определить две вершины в качестве входной и выходной, при этом вершины находятся в разных подграфах. Тогда для каждого подграфа требуется построить вспомогательный граф и найти кратчайшие пути до вершин пересечения подграфов, после чего возможно составить итоговые найденные пути на исходном графе.

Для наглядного представления алгоритма двунаправленного поиска путей на графе возьмем неориентированный граф с 8 вершинам, изображенный на рисунке 1. Построим пути от вершины 1, до вершины 8 с ограничением метрики 4.

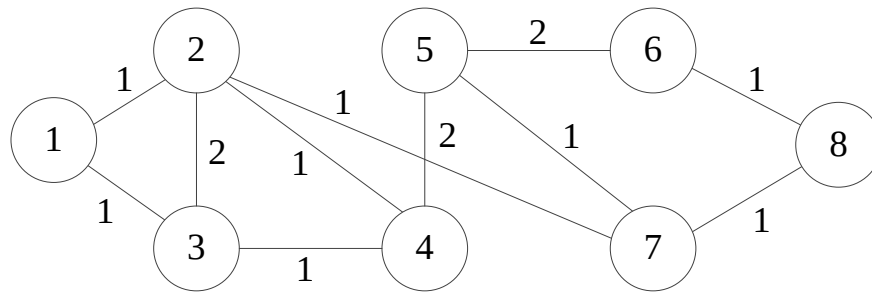


Рисунок 1 – Граф программно-конфигурируемой сети связи

Тогда, исходя из описания разработанного алгоритма, построим два вспомогательных графа, имеющих порожденные пути через вершины 4-5 и 2-7. Тогда исходная задача сводится к нахождению путей от вершин 1 и 8 к вершинам 2,4 и 5,7 соответственно.

На рисунке 2 показаны построенные вспомогательные графы с указанием возможных путей передачи данных

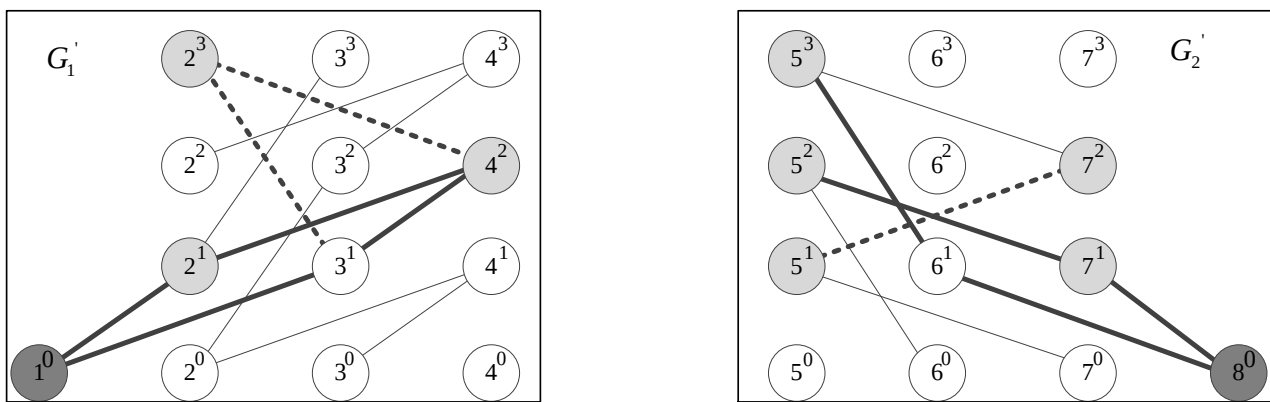


Рисунок 2 – Двухнаправленный поиск путей с построением вспомогательных графов

В результате работы алгоритма двухнаправленного поиска в каждом вспомогательном графе найдены искомые пути. Для G_1' такими являются: 1-2:1; 1-3-2:3; 1-3-4-2:3; 1-3-4:2; 1-2-4:2. Для G_2' : 8-7:1, 8-6-5:3, 8-7-5:2. Поскольку существуют порожденные пути 2-7 и 4-5, то конечное решение задачи – составление путей из обоих подмножеств, суммарная метрика которых не превысит 4, ввиду начального ограничения.

При этом временная сложность алгоритма может быть выражена через:

$$O(q_1 S_{m1} D_1 \cdot \log(S_{m1} D_1) + q_2 S_{m2} D_2 \cdot \log(S_{m2} D_2)) \quad (1)$$

где q_i – количество путей, S_{mi} – средняя степень вершин, D_i – длина максимального пути для подграфов, что эквивалентно $\sum O(q_i E_i \cdot \log E_i)$ примем, что количество искомых маршрутов с использованием разработанного метода двухнаправленного поиска на основе построения вспомогательных подграфов и алгоритма Йена эквивалентна.

Тогда временная сложность двухнаправленного поиска может быть представлена в виде $O\left(E \cdot \log\left(\frac{E}{2}\right)\right)$. Кроме этого необходимо учесть сложность построения вспомогательного графа и деления графа пополам. Для первого случая добавочный компонент к временной сложности может быть представлен как $O(E \cdot D)$, где D – параметр задержки передачи данных в искомых путях, а для деления графа – E . Условие применения разработанных методов может быть выражено неравенством:

$$O(qDE \cdot \log(DE)) < O(qV(E + V) \cdot \log V), \quad (2)$$

упростив которое получим:

$$D < V \left(1 + \frac{V}{E}\right). \quad (3)$$

В случае разреженного графа $E \approx V$, тогда выражение 3 принимает форму $D < 2V$, то есть поиск путей с использованием вспомогательного графа актуально для поиска множества маршрутов с низкой задержкой передачи данных. При рассмотрении более плотных графов условие стремится к $D < V$, что позволяет применять его в высокосвязных ПКС топологиях, например Spine-Leaf. Тогда справедливо, что в условиях разреженного графа $\log\left(\frac{E}{2}\right) \approx \log V$, следовательно, сложность разработанного алгоритма составит 50% от известного, поскольку исходный граф разделен пополам для построения вспомогательных графов.

Реальное время работы алгоритма при этом будет зависеть от множества факторов, зависящих от конкретной программной реализации, поскольку процедуры записи, модификации, хранения информации и добавления вершин и ребер в граф имеют свою временную и алгоритмическую сложности, разную для используемых способов хранения данных: списка смежности, списка инцидентности, матрицы смежности и т.д. Общей же тенденцией остается увеличение сложности при повышении размерности графа, аналогично типовым алгоритмам поиска путей на графе.

Заключение

В работе рассмотрена проблема поиска множества путей передачи данных на графе, возможность использования данных ПКС контроллера в качестве исходных данных для решения указанной проблемы. Предложено решение задачи поиска множества путей на графе, выраженное в введении дополнительного функционала в алгоритм поиска путей с использованием вспомогательного графа, а именно, использование двунаправленного поиска.

Разработанное решение позволяет находить множество путей передачи данных, в том числе пересекающихся, что отличает его от множества известных алгоритмов. Рассмотрен пример поиска путей на графе, а также приведена расчетная временная сложность алгоритма. При этом алгоритм двунаправленного поиска путей с построением вспомогательных графов имеет до 50% меньшее значение расчетной временной сложности, чем алгоритм без двунаправленного поиска.

Литература

1. Терешкевич А. А., Зубалов А. Н. Обзор технологии " Программно-конфигурируемые сети ПКС/SDN" //Газовая промышленность. – 2016. – №. 12 (746). – С. 64-71.
2. Никишин К. И. Исследование и моделирование таблицы потоков коммутатора Openflow в программноконфигурируемых сетях //Вестн. Рязанского государственного радиотехнического университета. – 2022. – №. 81. – С. 42-50.
3. Корячко В. П., Перепелкин Д. А., Цыганов И. Ю. Реализация подхода сетевого слайсинга в программно-конфигурируемых сетях на основе qos-маршрутов //Новые информационные технологии в научных исследованиях. – 2020. – С. 104-106.
4. Лесных Е. Ю. Построение оптимального сетевого графа //Электронный периодический рецензируемый научный журнал «SCI-ARTICLE. RU». – 2017. – С. 166.
5. Бурдонов И. Б., Евтушенко Н. В., Косачев А. С. Безопасная реализация виртуальной сети на плоскости данных SDN //Труды Института системного программирования РАН. – 2021. – Т. 33. – №. 1. – С. 123-136.

DEVELOPMENT OF A BIDIRECTIONAL PATH-FINDING ALGORITHM IN SOFTWARE-DEFINED NETWORKS

A.E. Baskakov, Lecturer

National Research University of Electronic Technology (MIET)

The core concept of Software-Defined Networking lies in the utilization of a centralized controller to gather detailed topology data via the OpenFlow protocol. Representing the communication structure as an undirected weighted graph allows for the consideration of bandwidth and latency for each edge. The proposed method addresses the problem of identifying a set of overlapping routes by constructing auxiliary graphs. A distinctive feature of the suggested approach is its ability to find intersecting paths, a task that remains challenging when using classical iterative algorithms. Theoretical analysis of time complexity has demonstrated that, in sparse graph environments, the proposed method can reduce computational overhead by up to 50% compared to traditional solutions. Furthermore, the efficiency conditions for the algorithm have been formulated based on latency parameters and the density of topology links.



ВАРИАНТ ПОСТРОЕНИЯ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ КОМПЛЕКСНЫХ ЧИСЕЛ

проф. Жук А.П.

Северо-Кавказский федеральный университет

Рассмотрена структура генератора псевдослучайных последовательностей исключительно комплексных чисел, мнимая часть которых отлична от нуля. Принцип формирования псевдослучайных комплексных чисел реализован путем объединения двух независимых псевдослучайных последовательностей действительных чисел, при этом из выходной последовательности исключаются значения, для которых мнимая часть равна нулю. Показан принцип формирования псевдослучайных комплексных чисел разработанным генератором. Особенностью рассматриваемого генератора является использование механизма логического управления, позволяющего исключить появление значений с нулевой мнимой частью в выходной последовательности псевдослучайных комплексных чисел.

Комплексные числа широко применяются в современной вычислительной технике, системах цифровой обработки сигналов и телекоммуникационных технологиях. Использование комплексного представления сигналов позволяет одновременно учитывать амплитудные и фазовые характеристики гармонических процессов, что особенно важно при анализе и моделировании сигналов в радиотехнических системах [1-3].

В задачах цифровой обработки сигналов, криптографии и моделирования часто используются псевдослучайные последовательности. Такие последовательности формируются детерминированными алгоритмами, но обладают статистическими свойствами случайных процессов. Псевдослучайные числа применяются при моделировании шумовых сигналов, тестировании цифровых систем, а также при формировании специальных сигнальных последовательностей [3].

При решении задач формирования сигналов на основе псевдослучайных исходных данных, требуется применение не только генераторов псевдослучайных чисел, но и генераторов псевдослучайных комплексных чисел. При этом появление в последовательности псевдослучайных комплексных чисел элементов с нулевой мнимой частью является нежелательным, поскольку они в этом случае фактически становятся действительными числами и могут нарушать структуру последовательности.

Целью статьи является исследование структуры и принципа функционирования генератора псевдослучайных комплексных чисел, обеспечивающего формирование псевдослучайной последовательности без действительных значений, а также возможных областей его применения.

В работе [4] предложено техническое решение, обеспечивающее формирование последовательности, состоящей исключительно из комплексных чисел, мнимая часть которых отлична от нуля. Устройство использует два генератора псевдослучайных чисел и механизм логического управления, позволяющий исключить появление действительных элементов в выходной последовательности.

Геометрически каждое комплексное число может быть представлено точкой на комплексной плоскости с координатами (a, b) . Если мнимая часть равна нулю, то комплексное число вырождается в действительное.

В задачах цифровой обработки сигналов и моделирования часто требуется формирование последовательностей чисел, обладающих свойствами случайности. Однако такие последовательности формируются детерминированными алгоритмами и поэтому называются псевдослучайными.

Одним из распространённых способов получения таких последовательностей является использование генераторов псевдослучайных чисел, функционирующих в конечных полях $GF(q)$. Подобные генераторы позволяют формировать последовательности с большим периодом и хорошими статистическими характеристиками.

Формирование псевдослучайных комплексных чисел может быть реализовано путем объединения двух независимых псевдослучайных последовательностей действительных чисел. В этом случае одна последовательность используется для формирования действительной части комплексного числа, а другая – для формирования его мнимой части.

Комплексное число в этом случае может быть представлено в виде

$$Z = a + bi = Ae^{i\varphi},$$

где a и b являются действительными элементами псевдослучайной последовательности комплексных чисел.

Генератор псевдослучайных комплексных чисел предназначен для формирования псевдослучайной последовательности комплексных чисел на основе двух независимых генераторов, функционирующих в конечном поле $GF(q)$. Согласно [1] генератор содержит первый и второй генераторы псевдослучайных чисел с линейной обратной связью, блок формирования комплексных чисел, инвертор и ключ.

Структурная схема генератора псевдослучайных комплексных чисел представлена на рисунке 1.

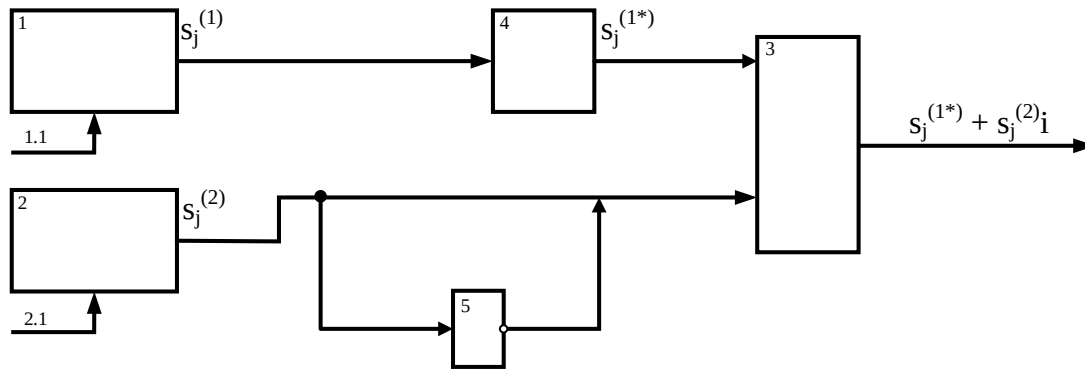


Рисунок 1 – Структурная схема генератора псевдослучайных комплексных чисел

Первый генератор псевдослучайных чисел формирует псевдослучайную последовательность $s_j^{(1)}$, предназначенную для действительной части комплексного числа. Второй генератор формирует последовательность $s_j^{(2)}$, используемую для построения мнимой части комплексного числа.

Выход первого генератора подключён к информационному входу ключа. Выход второго генератора подключён к входу блока формирования псевдослучайных комплексных чисел, а также к входу инвертора. Выход инвертора подключён к управляющему входу ключа.

Выход ключа соединён с первым входом блока формирования псевдослучайных комплексных чисел. Второй вход блока формирования соединён с выходом второго генератора.

В блоке формирования псевдослучайных комплексных чисел осуществляется формирование комплексного значения на основе действительной и мнимой составляющих.

Таким образом, структура генератора псевдослучайных комплексных чисел ориентирована на формирование комплексных чисел вида

$$Z_j = s_j^{(1)} + s_j^{(2)} i.$$

Механизм исключения действительных чисел реализуется следующим образом.

Значение, формируемое вторым генератором псевдослучайных чисел, поступает на вход инвертора. Если значение равно нулю, инвертор формирует управляющий сигнал, размыкающий ключ. В этом случае значение действительной части не передается в блок формирования комплексного числа.

Если значение второго генератора отлично от нуля, то ключ замыкается, и действительная составляющая передается в блок формирования псевдослучайных комплексных чисел. В результате формируется комплексное число.

Таким образом из выходной последовательности исключаются значения, для которых мнимая часть равна нулю. Это обеспечивает формирование последовательности, состоящей исключительно из комплексных чисел.

Одной из возможных областей применения является цифровая обработка сигналов. В таких системах комплексное представление сигналов используется при анализе спектральных характеристик, моделировании сигналов и разработке алгоритмов обработки информации [1, 3].

Генераторы псевдослучайных комплексных чисел также могут использоваться при моделировании различных процессов в вычислительных системах. Псевдослучайные комплексные последовательности позволяют имитировать шумовые воздействия и случайные сигналы, что важно при исследовании устойчивости алгоритмов и систем обработки данных [2].

Кроме того, подобные генераторы могут применяться в криптографических системах и системах защиты информации. Псевдослучайные последовательности используются для формирования ключей, маскирования данных и построения различных криптографических алгоритмов.

Также генераторы псевдослучайных комплексных чисел могут использоваться при тестировании цифровых устройств и программных систем. Использование комплексных последовательностей позволяет проводить более точное моделирование процессов обработки сигналов и оценивать работу различных алгоритмов в условиях случайных воздействий.

Таким образом, генератор псевдослучайных комплексных чисел может находить применение в широком

спектре задач цифровой обработки сигналов, моделирования, криптографии и тестирования вычислительных систем.

По результатам изложенного выше, сформулируем следующие выводы:

В работе описана структура генератора псевдослучайных комплексных чисел и проанализирован принцип его функционирования. Показано, что устройство использует два генератора псевдослучайных чисел для формирования действительной и мнимой составляющих комплексного значения.

Особенностью рассматриваемого генератора является использование механизма логического управления, позволяющего исключить появление значений с нулевой мнимой частью в выходной последовательности псевдослучайных комплексных чисел.

Рассмотрены возможные области применения генератора псевдослучайных комплексных чисел, включая задачи цифровой обработки сигналов, моделирования и криптографических систем.

Литература

1. Сухарев Е.М. Общесистемные вопросы защиты информации: коллективная монография / Е.М. Сухарев [и др.]. Кн.1 – М.: Радиотехника, 2003. –296 с.
2. Помехозащищённость систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью [Текст] / В.И. Борисов, В.М. Зинчук, А.Е. Лимарев, Н.П. Мухин, Г.С. Нахмансон; Под ред. В.И. Борисова. – М.: Радио и связь, 2003. – 640 с.: ил. 314.
3. Жук А.П. Защита информации / А.П. Жук, Е.П. Жук, О.М. Лепешкин., А.И. Тимошкин. - Москва: ИЦ РИОР, 2021. - 400 с. - ISBN 978-5-369-01759-3. - URL: <https://ibooks.ru/bookshelf/361250/reading> (дата обращения: 10. 02.2026).
4. Патент № 2848175 Российская Федерация, МПК G06F 7/58 (2006.01). Генератор псевдослучайных комплексных чисел : № 2025103439: заявл. 17.02.2025; опубл. 16.10.2025 / Жук А.П., Макаров И.В., Небеская М.В., Доскиев Р.М., Жук Е.П., Стогний К.В.; заявитель ФГАОУ ВО «Северо-Кавказский федеральный университет». 14 с.: ил. // Реестр изобретений Российской Федерации. URL: https://www1.fips.ru/registers-doc-view/fips_servlet?DB=RUPAT&rn=9209&DocNumber=2848175&TypeFile=html (дата обращения: 09.04.2026).

A VERSION FOR CONSTRUCTING A PSEUDO-RANDOM COMPLEX NUMBER GENERATOR

professor Zhuk A.P.

North-Caucasus Federal University

The structure of a pseudorandom sequence generator for exclusively complex numbers with a nonzero imaginary part is examined. The principle of generating pseudorandom complex numbers is implemented by combining two independent pseudorandom sequences of real numbers, with values for which the imaginary part is zero excluded from the output sequence. The principle of generating pseudorandom complex numbers using the developed generator is demonstrated. A distinctive feature of this generator is its use of a logical control mechanism, which eliminates the occurrence of values with a zero imaginary part in the output sequence of pseudorandom complex numbers.



АТМОСФЕРНАЯ ОПТИЧЕСКАЯ СВЯЗЬ (FSO) ДЛЯ БЕСПИЛОТНЫХ АППАРАТОВ: ЭКСПЕРИМЕНТАЛЬНОЕ МОДЕЛИРОВАНИЕ И ПУТИ МОДЕРНИЗАЦИИ.

асп. Кадочников Д.М.¹, проф., доц., д.т.н. Страхов С.Ю.¹,
доц., к.т.н. Сотникова Н.В.¹, к.т.н. Брусенцов К.А.²

¹Балтийский государственный технический университет «Военмех» им. Д. Ф. Устинова
²ООО «Пантес МТ»

В статье исследуются методы организации атмосферной оптической связи (FSO) для роев беспилотных летательных аппаратов. Проведен сравнительный анализ макетов лазерного (650 нм) и светодиодного (850 нм) каналов с использованием аналитических моделей оптического бюджета трассы. Экспериментально доказано, что светодиодные системы эффективны на малых дистанциях за счет радикального снижения требований к наведению, тогда как лазерные обеспечивают высокую скрытность и дальность, но уязвимы к фоновой засветке и ошибкам позиционирования. Для преодоления выявленных ограничений предложена концептуальная модернизация архитектуры под современные отраслевые стандарты: переход на длину волны 1550 нм, внедрение лавинных фотодиодов, энергоэффективной PPM-модуляции, компактных систем отклонения луча на базе MEMS-зеркал и алгоритмов помехоустойчивого кодирования LDPC.

Развитие современных автономных систем и интенсификация использования групп беспилотных летательных аппаратов (БПЛА) требуют создания новых методов обмена данными, способных обеспечить высокую пропускную способность в условиях радиоэлектронного противодействия и дефицита доступного радиочастотного спектра. В этом контексте передача данных с помощью оптического и лазерного излучения (Free Space Optics, FSO) рассматривается как одна из наиболее перспективных альтернатив традиционной радиосвязи. Основными преимуществами FSO-систем являются высокая скрытность канала, невосприимчивость к электромагнитным помехам, отсутствие необходимости лицензирования частотного диапазона и потенциал для достижения скоростей передачи свыше 1 Гбит/с [1].

Ключевой особенностью лазерного канала связи является узкая направленность излучения, которая обеспечивает высокую энергетическую эффективность и защиту от перехвата информации. Однако практическая реализация таких линий связи на подвижных платформах сталкивается с серьезной технической проблемой — необходимостью наведения и непрерывного удержания луча на апертуре приемника (Pointing, Acquisition, and Tracking — PAT). В условиях динамичного маневрирования БПЛА, влияния вибраций и атмосферной турбулентности создание систем PAT требует значительных вычислительных и энергетических затрат, что вступает в противоречие с жесткими массогабаритными и энергетическими ограничениями (SWaP-характеристиками) малых автономных аппаратов [2].

Для решения задач информационного обмена на относительно малых дистанциях (до нескольких сотен метров) рациональной альтернативой лазерным системам выступает использование некогерентных источников излучения, в частности, светодиодов. Переход к оптическому каналу с большей угловой расходимостью позволяет существенно снизить требования к точности юстировки и стабильности систем наведения. Несмотря на закономерное снижение интенсивности излучения в зоне приема и уменьшение скрытности канала по сравнению с лазером, такие системы обеспечивают более высокую надежность соединения в условиях интенсивного взаимного перемещения абонентов, сохраняя при этом преимущества электромагнитной совместимости.

В данной работе авторами проводится сравнительный анализ характеристик лазерного и оптического (светодиодного) каналов связи на основе разработанной масштабированной физической модели. В ходе исследования выполнено экспериментальное моделирование двух типов линий связи: на базе инфракрасного светодиода с амплитудной манипуляцией и узконаправленного полупроводникового лазера. Целью работы является количественная оценка ключевых эксплуатационных параметров — предельной дальности связи, вероятности битовой ошибки (BER) и устойчивости к фоновым помехам. Полученные результаты позволяют обосновать выбор оптимальной архитектуры приемопередающего тракта для практических задач ближней связи в мобильных робототехнических комплексах.

Для аналитического обоснования ограничений рассматриваемых систем необходимо опираться на математическую модель энергетического бюджета трассы. Мощность оптического сигнала на входе приемника P_{rx} может быть выражена уравнением:

$$P_{rx} = P_{tx} * \frac{A_{rx}}{\pi \left(\frac{\theta L}{2}\right)^2} * \tau_{atm} * \tau_{opt} \text{ Вт},$$

где P_{tx} — мощность передатчика, A_{rx} — эффективная площадь апертуры фотоприемника, θ — угол расходимости излучения, L — дальность связи, а τ_{atm} и τ_{opt} — коэффициенты пропускания атмосферы и оптической системы соответственно.

Данное выражение наглядно демонстрирует квадратичную зависимость потерь от угла расходимости, математически объясняя резкое падение дальности при переходе от лазера к светодиоиду. Влияние среды передачи, включая метеорологические осадки и аэрозоли, описывается законом Бугера-Ламберта-Бера, согласно которому атмосферное пропускание τ_{atm} .

$$\tau_{atm} = e^{-\sigma L},$$

где σ — коэффициент экстинкции, зависящий от длины волны и концентрации рассеивающих частиц.

Качество цифровой связи определяется вероятностью битовой ошибки (BER). Для применяемой в эксперименте простейшей амплитудной манипуляции (OOK, On-Off Keying) теоретический предел вероятности ошибки вычисляется как:

$$BER = \frac{1}{2} * \operatorname{erfc} \left(\frac{\sqrt{SNR}}{2\sqrt{2}} \right),$$

где SNR — отношение сигнал/шум, зависящее от принятой мощности P_{rx} и уровня тепловых и дробовых шумов фотодетектора.

Сравнение экспериментальных значений BER с этой теоретической функцией позволяет оценить степень деградации сигнала из-за фоновой засветки и инерционности компонентов.

Экспериментальная апробация проводилась на лабораторном стенде, моделирующем два типа каналов. Оптический (светодиодный) модуль был реализован на базе инфракрасного диода с длиной волны 850 нм и выходной мощностью 20 мВт, управляемого микроконтроллером с генерацией несущей частоты 38 кГц и применением ООК-модуляции. Приемный тракт состоял из кремниевого фотодиода с ИК-фильтром, двухкаскадного усилителя и узкополосного фильтра, настроенного на несущую частоту, с последующим пиковым детектированием.

Лазерный канал базировался на коллимированном полупроводниковом модуле (650 нм, 1 мВт, расходимость 2 мрад), обеспечивающем формирование пятна диаметром около 10 мм на дистанции 5 метров. Модуляция осуществлялась прямым управлением током лазера (до 20 кГц). Приемник лазерного излучения был построен на базе кремниевого фототранзистора, сигнал с которого проходил через RC-фильтр нижних частот на компаратор с регулируемым гистерезисом для повышения помехоустойчивости.

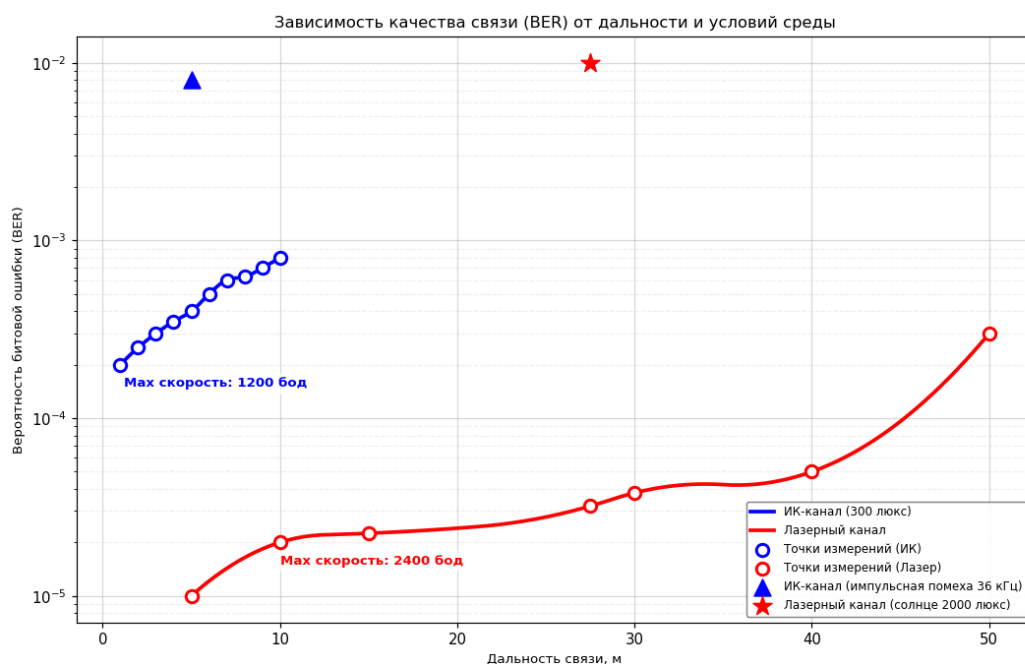


Рисунок 1 — Результаты испытаний подтвердили теоретические предположения о влиянии расходимости луча и аппаратной инерционности на характеристики связи.

Результаты испытаний, представленные на рисунке 1, подтвердили теоретические предположения о влиянии расходимости луча и аппаратной инерционности на характеристики связи. Инфракрасный светодиодный канал продемонстрировал устойчивость к взаимному смещению приемопередатчиков на дистанциях до 5 метров. При уровне искусственного освещения 300 люкс значение BER на расстоянии 1 метр составило $2 \cdot 10^{-4}$, а при увеличении дальности до 5 метров деградировало до $8 \cdot 10^{-4}$. Воздействие импульсной ИК-помехи с частотой 36 кГц приводило к росту BER до $8 \cdot 10^{-3}$ из-за спектрального перекрытия. Максимальная скорость передачи была ограничена 1200 бод, что обусловлено пакетированием ошибок из-за инерционности аналоговых цепей пикового детектора. Лазерная система, напротив, обеспечила дальность уверенного приема до 70 метров при угловом отклонении не более $\pm 0,5^\circ$. В затемненном помещении на дистанции 5 метров BER лазерного канала достигал 10^{-5} , а при проведении испытаний на улице на дистанции 50 метров — $3 \cdot 10^{-4}$. Скорость передачи составила 2400 бит/с. Ошибки в лазерном канале носили равномерный одиночный характер. Главной уязвимостью лазерной установки оказалась чувствительность к прямой солнечной засветке: при освещенности 2000 люкс происходило насыщение фототранзистора, и BER резко ухудшался до 10^{-2} .

Для адаптации подобных решений к современным задачам роевой робототехники требуется переход от макетной компонентной базы к актуальным технологиям атмосферной оптики. Во-первых, использование видимого диапазона (650 нм) нерационально из-за высокой чувствительности к солнечному свету и демаскирующего эффекта; стандартом для современных систем FSO является использование длин волн 1550 нм или 905/1064 нм, что повышает безопасность для зрения и снижает влияние атмосферного рассеяния. Во-вторых, для преодоления частотных ограничений необходимо отказаться от инерционных фототранзисторов в пользу лавинных фотодиодов (APD) или быстродействующих PIN-фотодиодов в связке с трансимпедансными усилителями (TIA), что позволит поднять скорость передачи до мегабитных и гигабитных значений. В-третьих, ООК-модуляция может быть заменена на фазово-импульсную модуляцию (PPM), которая является стандартом де-факто для оптической связи в условиях дефицита энергии, или на методы ортогонального частотного разделения (OFDM) для светодиодных систем связи (Li-Fi) [3]. Кроме того, проблема узконаправленности лазерного луча на подвижных носителях сегодня решается внедрением систем быстрого отклонения луча на базе микроэлектромеханических систем (MEMS-зеркал) или быстрых управляемых зеркал (FSM), что исключает необходимость механического поворота всего аппарата [4]. Наконец, для борьбы с флуктуациями сигнала из-за атмосферной турбулентности требуется внедрение современных алгоритмов прямой коррекции ошибок (FEC), таких как коды с малой плотностью проверок на четность (LDPC) или коды Рида-Соломона [3,5].

Проведенное исследование доказывает, что при малых расстояниях и сложно прогнозируемом движении абонентов применение широкоугольного светодиодного канала оправдано благодаря радикальному упрощению подсистемы наведения. При росте требований к дальности, пропускной способности и конфиденциальности передаваемых данных безальтернативным становится лазерный канал. Дальнейшее развитие систем оптической бесконтактной связи должно опираться на комплексный подход, включающий переход на инфракрасный диапазон 1550 нм, применение высокоскоростной оптоэлектроники, энергоэффективных методов модуляции и алгоритмических методов коррекции ошибок. Сочетание этих решений позволит создать надежные системы информационного обмена, отвечающие жестким требованиям современных автономных мобильных комплексов.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации (НИР «Разработка и исследование методов управления группами автономных беспилотных летательных аппаратов на основе перспективных систем информационного обеспечения и взаимодействия между отдельными аппаратами в группе», FZWF-2024-0002).

Литература

1. Страхов С.Ю., Савин А.В., Сотникова Н.В., Орлов А.Е. Оценка влияния оптических неоднородностей атмосферы на точность позиционирования лазерного луча при вертикальном зондировании // Оптический журнал. 2025. Т. 92. № 2. С. 56–66. <http://doi.org/10.17586/1023-5086-2025-92-02-56-66>
2. Крылова М.А., Сотникова Н.В., Страхов С.Ю. Электромагнитное моделирование распределенной антенной решетки на основе роя беспилотных летательных аппаратов // Современные проблемы

- радиоэлектроники и телекоммуникаций : сб. науч. тр. / под ред. И. Л. Афолина. — Москва-Севастополь : Изд-ва : РНТОРЭС им. А.С. Попова, СевГУ, 2024. — № 7. — 236 с.
3. Краснов Р. П. Система атмосферной оптической связи OFDM-типа на базе кода LDPC с перемежением в турбулентном канале // Вестник Воронежского государственного технического университета. — 2018. — Т. 14, № 4. — С. 71–76. (Источник добавлен для обоснования применения помехоустойчивых кодов)
 4. Abdelfatah R., Alshaer N. A., Ismail T. A review on pointing, acquisition, and tracking approaches in UAV-based FSO communication systems// Optical and Quantum Electronics. — 2022. — Vol. 54, № 9. — P. 571.
 5. Gupta A., Dhawan D., Gupta N. Review on UAV-based FSO links: recent advances, challenges, and performance metrics// Optical Engineering. — 2024. — Vol. 63, № 4. — P. 041204.

FREE-SPACE OPTICS (FSO) FOR AUTONOMOUS VEHICLES: EXPERIMENTAL MODELING AND MODERNIZATION STRATEGIES.

Postgraduate student Kadochnikov D.M.¹,
Prof., Assoc., Doctor of Technical Sciences Strakhov S.Yu.¹,
Assoc., Candidate of Technical Sciences Sotnikova N.V.¹,
Candidate of Technical Sciences Brusentsov K. A.²

¹Baltic State Technical University "Voenmeh" named after D. F. Ustinov

²Pantes MT LLC

This article examines methods for organizing free-space optical (FSO) communication for swarms of unmanned aerial vehicles. A comparative analysis of laser (650 nm) and LED (850 nm) channel configurations was conducted using analytical models of the optical path budget. Experiments have shown that LED systems are effective at short distances due to a significant reduction in alignment requirements, whereas laser systems provide high stealth and range but are vulnerable to background light and positioning errors. To overcome the identified limitations, a conceptual upgrade of the architecture to meet modern industry standards is proposed: a transition to a wavelength of 1550 nm, the introduction of avalanche photodiodes, energy-efficient PPM modulation, compact beam deflection systems based on MEMS mirrors, and LDPC error-correcting coding algorithms.



БЕСПРОВОДНЫЕ ДАТЧИКИ С ОПТИЧЕСКИМ СПОСОБОМ ПЕРЕДАЧИ ИНФОРМАЦИИ В СИСТЕМАХ МОНИТОРИНГА ОБЪЕКТОВ

асп. Казанков А.А.^{1,2}, д.т.н. Сергеев В.А.²,
к.т.н. Фролов И.В.², асп. Кузьмин Н.П.¹, к.т.н. Радаев О.А.²

¹ Ульяновский государственный технический университет

² Ульяновский филиал Института радиотехники и электроники им. В.А. Котельникова
Российской академии наук

В работе рассматриваются принципы построения беспроводных датчиков с оптическим способом передачи информации, предназначенных для систем мониторинга объектов и интеллектуальных систем управления. Проведен анализ современных технологий беспроводной передачи данных, применяемых в сенсорных сетях, а также рассмотрены ограничения традиционных радиочастотных протоколов, связанные с высокой нагрузкой диапазонов частот и проблемами электромагнитной совместимости. Показана перспективность применения оптических каналов связи для повышения помехоустойчивости и надежности передачи информации. Предложены и описаны варианты построения беспроводных датчиков температуры на основе микросхемы триггера Шмитта и специализированной микросхемы NST1001 с оптическим каналом передачи данных. Представлены два варианта разделения сигналов от пространственно разнесенных датчиков: адресно-временное разделение при передаче информации на одной длине волны и спектральное разделение каналов по длине волны оптического излучения с использованием светодиодов различных спектральных диапазонов и фотоприемников с оптическими фильтрами. Выполнен сравнительный анализ предложенных методов разделения сигналов и определены особенности их практической реализации.

Современное развитие технологий автоматизации и «Интернета вещей» способствует активному внедрению интеллектуальных систем управления как жилыми, так и нежилыми помещениями (объектами). Концепция «умного дома» предполагает интеграцию множества датчиков, исполнительных устройств и вычислительных модулей в единую информационно-управляющую среду. Основной задачей таких систем является повышение комфорта проживания, энергоэффективности и безопасности. Основными узлами систем мониторинга являются датчики (температуры, влажности, освещенности и др.) [1, 2].

Традиционно в системах умного дома для передачи информации между устройствами используются радиочастотные технологии: Wi-Fi, ZigBee, Bluetooth, Z-Wave и LoRaWAN [2]. Несмотря на широкое распространение перечисленных технологий, в настоящее время наблюдается существенная проблема высокой загрузки радиочастотного спектра, особенно в диапазоне 2,4 ГГц, который одновременно используется устройствами Wi-Fi, Bluetooth, ZigBee, бытовой электроникой и промышленными системами связи. Увеличение количества беспроводных устройств приводит к росту уровня электромагнитных помех, возникновению коллизий при передаче данных и снижению стабильности работы сетей связи.

Дополнительной проблемой является обеспечение электромагнитной совместимости интеллектуальных устройств, особенно в условиях плотной городской застройки и большого количества радиоэлектронных средств. Воздействие внешних электромагнитных полей может вызывать ухудшение качества связи, потерю пакетов данных и снижение надежности функционирования системы «умного дома».

В связи с этим особую актуальность приобретают альтернативные способы беспроводной передачи информации, в частности оптические методы связи. Использование инфракрасного, видимого или лазерного излучения позволяет существенно снизить влияние электромагнитных помех, повысить информационную безопасность и обеспечить устойчивую работу сенсорных сетей в условиях высокой загрузки радиочастотного спектра.

Целью данной работы является исследование особенностей построения беспроводных датчиков с оптическим способом передачи информации в системе управления «умным домом», а также анализ преимуществ и ограничений данной технологии.

1. Датчик температуры на триггере Шмитта

Датчик температуры с импульсным выходом и оптическим каналом передачи оптической информации был собран по схеме мультивибратора на триггере Шмитта SN74LVC1G14DBVR (рисунок 1). Термочувствительным элементом является терморезистор R1 с номинальным сопротивлением 10 кОм при температуре 25 °С. Светодиод VD1 типа SIR0805CS с длиной волны в максимуме спектра излучения 940 нм используется для преобразования электрических колебаний на выходе датчика, в импульсное оптическое излучение. Принцип работы датчика поясняется временными диаграммами, представленными на рисунке 2.

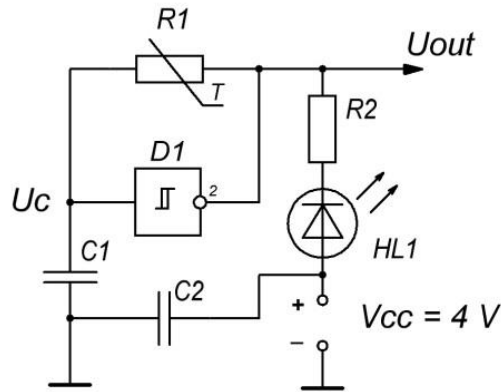


Рисунок 1 - Схема электрическая принципиальная датчика температуры на триггере

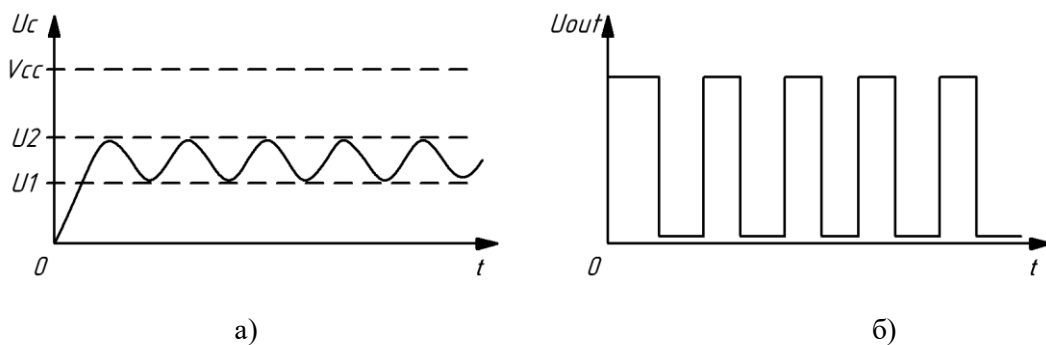


Рисунок 2 - Временная диаграмма напряжения на конденсаторе C1 (а) и выходного напряжения (б) датчика температуры на триггере

В начальный момент времени конденсатор C1 номиналом 470 нФ не заряжен и на входе триггера Шмитта – уровень логического нуля, соответственно на выходе триггера – логическая единица, светодиод HL1 выключен. Через терморезистор R1 начинает протекать ток, под действием которого конденсатор C1 заряжается. При достижении напряжения на конденсаторе C1 уровня верхнего порога переключения триггера (U2) выходное напряжение триггера переходит в состояние логического нуля, светодиод включается. Ток светодиода ограничивается резистором R2 с сопротивлением 1 кОм и составляет 2 мА. Далее начинается разряд конденсатора C1 через терморезистор R1. При достижении напряжения на конденсаторе уровня нижнего порога переключения триггера (U1) триггер переключается в состояние логической единицы, светодиод выключается. Снова начинается заряд конденсатора до уровня U2. Далее процесс повторяется периодически. Таким образом, оптический сигнал светодиода представляет собой последовательность прямоугольных импульсов с частотой, определяемой параметрами частотозадающих элементов схемы:

$$f = \frac{1}{0.5R_1C_1} \quad (1)$$

При температуре 25 °С и частота импульсов составляет 600 Гц.

Поскольку сопротивление терморезистора уменьшается при увеличении температуры, частота колебаний автогенератора увеличивается. Зависимость частоты колебаний автогенератора от температуры, измеренная в диапазоне от 25 °С до 100 °С при размещении датчика в термостате CH3-150 Combitherm, приведена на рисунке 3.

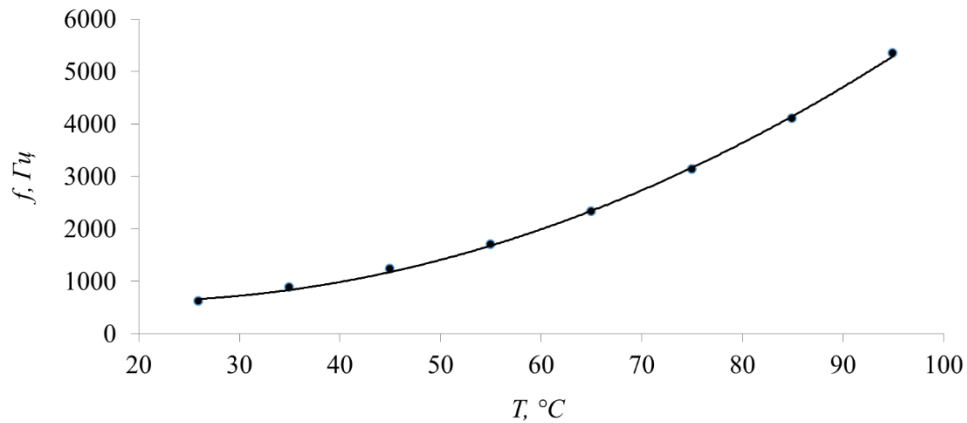


Рисунок 3 - Функция преобразования температуры в частоту колебаний мультивибратора на триггере

Видно, что зависимость $f(T)$ нелинейная и удовлетворительно описывается полиномом второй степени:

$$f_{Hz}(T_{°C}) = 0.801T^2 - 29.789T + 894.98 \quad (2)$$

2. Датчик температуры на микросхеме NST1001

В качестве чувствительного элемента датчика температуры с импульсным выходом может быть использована микросхема NST1001-QDNR серии D-NTC® компании NOVOSENSE Microelectronics [3] с габаритными размерами 0,8×1,6 мм. Микросхема имеет высокую точность и разрешающую способность в диапазоне температур от -50 до 150 °С и пригодна для применения в качестве датчика температура окружающей среды.

Микросхема NST1001 имеет встроенный фильтр электромагнитных помех, что позволяет использовать его в устройствах с высоким уровнем помех и в беспроводных узлах датчиков IoT с особенно строгими требованиями к питанию. Из-за очень низкого рабочего тока подключение датчика возможно как напрямую к выводам GPIO микроконтроллера (рисунок 4,а), так и напрямую к светоизлучающим диодам при реализации оптического канала передачи информации (рисунок 4,б).

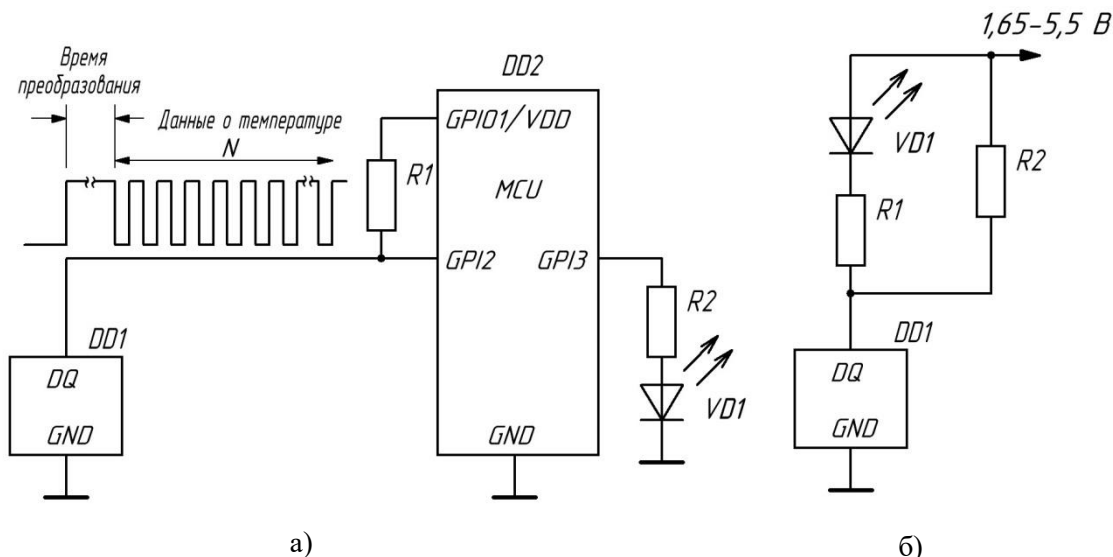


Рисунок 4 - Схема включения датчика NST1001-QDNR: с микроконтроллером (а), с без микроконтроллера (б)

Выходной сигнал датчика, снимаемый с вывода питания DQ, имеет импульсный характер и представляет собой последовательность электрических импульсов, количество которых N за заданный интервал времени пропорционально значению измеряемой температуры.

Основные технические характеристики микросхемы NST1001-QDNR:

- среднее время одного измерения с передачей данных 50 мс;
- погрешность измерения значений температуры в диапазонах
- 20°C ~ 85°C : ±0,5°C (макс.),
- 50°C ~ 150°C : ±0,75°C (макс.);
- разрешающая способность 0,0625°C;
- напряжение питания 1,65 – 5,5 В.

Температура определяется по калибровочной зависимости:

$$T = 0,0625 \cdot N - 50,0625 \text{ }^{\circ}\text{C} \quad (3)$$

3. Способы разделения сигналов от пространственно разнесенных датчиков

При построении беспроводной сенсорной системы с оптическим способом передачи информации одной из основных задач является обеспечение корректного разделения сигналов, поступающих от нескольких пространственно разнесенных датчиков температуры. Для решения данной задачи предлагаются два возможных варианта организации передачи данных.

В первом варианте передача информации от всех датчиков осуществляется на одной длине волны оптического излучения. В данном случае каждый датчик строится по структурной схеме, представленной на рисунке 4а, и содержит: чувствительный элемент, микроконтроллер, оптический передатчик на основе инфракрасного светодиода.

Чувствительный элемент выполняет измерение температуры в локальной зоне контроля. Далее микроконтроллер осуществляет преобразование измеренного значения в цифровой код, формирует информационный пакет и добавляет служебную информацию, содержащую адрес датчика. После этого данные передаются посредством инфракрасного оптического излучения.

Прием информации осуществляется централизованным фотоприемным устройством. В качестве приемного элемента используется фотодиод инфракрасного диапазона длин волн, преобразующий оптический сигнал в электрический. Полученный сигнал поступает на усилитель и полосовой фильтр, обеспечивающие повышение отношения сигнал/шум и подавление внешних помех. Далее сигнал подается в блок преобразования и микроконтроллер фотоприемного устройства, где производится декодирование информации и выделение адреса передающего датчика. После обработки данные передаются в центральный контроллер системы «умного дома».

В данном варианте разделение сигналов между датчиками осуществляется программно за счет применения адресации информационных пакетов, а также временного разделения передачи данных. Такой подход отличается сравнительно простой аппаратной реализацией и низкой стоимостью системы.

Во втором варианте разделение сигналов от пространственно разнесенных датчиков осуществляется по длине волны оптического излучения. Датчики строятся согласно схемам рисунка 1 или рисунка 4б. В каждом датчике применяется светодиод с определенным спектральным диапазоном излучения. Например, для различных датчиков могут использоваться: инфракрасные светодиоды с различной длиной волны, красные светодиоды, зеленые светодиоды, синие светодиоды.

В составе фотоприемного устройства применяются несколько фотодиодов с оптическими фильтрами, настроенными на соответствующие диапазоны длин волн. Каждый фотоприемный канал осуществляет прием сигнала только от определенного датчика. Таким образом, обеспечивается спектральное разделение каналов передачи информации, что позволяет существенно уменьшить вероятность взаимного влияния сигналов и повысить помехоустойчивость системы. Дополнительно такой подход позволяет реализовать одновременную передачу информации от нескольких датчиков без необходимости строгой временной синхронизации.

Метод разделения сигналов по длине волны обладает более высокой устойчивостью к коллизиям передачи данных по сравнению с временным разделением каналов, однако требует более сложной аппаратной реализации фотоприемного устройства и применения оптических фильтров [4, 5].

Сравнение двух предложенных вариантов показывает, что первый способ является более простым и экономичным, тогда как второй обеспечивает более высокую надежность и производительность системы при большом количестве одновременно работающих датчиков.

Заключение

Беспроводные датчики с оптическим способом передачи информации являются перспективным направлением развития систем управления умным домом. Их применение обеспечивает высокую помехоустойчивость, безопасность передачи данных и энергоэффективность, а также электромагнитную совместимость.

Наиболее эффективным является использование инфракрасного оптического диапазона в условиях помещений. Несмотря на существующие ограничения, связанные с необходимостью прямой видимости и

влиянием внешнего освещения, современные методы цифровой обработки сигналов позволяют существенно повысить надежность работы таких систем.

Работа выполнена при поддержке Российского научного фонда в рамках проекта № 23-91-06504.

Литература

1. Казанков, А. А. Устройство удаленного мониторинга системы отопления загородного дома / А. А. Казанков, Ю. П. Лавренова // Современные проблемы проектирования, производства и эксплуатации радиотехнических систем: Сборник научных трудов. – Ульяновск: Ульяновский государственный технический университет, 2025. – С. 199-203. – EDN QYPPBE.
2. Ершов, В. И. Возможности интеграции датчиков в систему умный дом под управлением протокола Zigbee / В. И. Ершов, Е. С. Фомина, В. Ю. Шалдыбин // Информационные технологии XXI века: Сборник научных трудов. – Хабаровск: Тихоокеанский государственный университет, 2024. – С. 112-117. – EDN CGKVME.
3. High-Accuracy 2-pins Digital Output Temperature Sensor with Pulse Count [Электронный ресурс]. – URL: <https://data.electronshtik.ru/z/Datasheet/ N/NST1001-QTZB.pdf> (дата обращения: 7.05.2026).
4. Патент № 2856848 С1 Российская Федерация, МПК G01J 5/48, G01J 5/10. Способ бесконтактного измерения температуры элементов конструкции электронного устройства: заявл. 28.08.2025; опубл. 25.02.2026 / А. М. Низаметдинов, В. А. Сергеев, И. В. Фролов [и др.]; заявитель Федеральное государственное бюджетное учреждение науки Институт радиотехники и электроники им. В.А. Котельникова Российской академии наук. – EDN BKFLEM.
5. Казанков, А. А. Датчик температуры с бесконтактным способом передачи информации / А. А. Казанков, Н. П. Кузьмин, В. А. Сергеев // Актуальные проблемы физической и функциональной электроники: Материалы 27-й Всероссийской молодежной научной конференции в рамках празднования 300-летия Российской академии наук, Ульяновск, 22–24 октября 2024 года. – Ульяновск: Ульяновский государственный технический университет, 2024. – С. 37-39. – DOI 10.61527/APPFE-2024.37-39. – EDN HEABAA.

WIRELESS SENSORS WITH AN OPTICAL METHOD OF INFORMATION TRANSMISSION IN OBJECT MONITORING SYSTEMS

Postgrad. student Kazankov A.A.^{1,2}, Prof. Sergeev V.A.², PhD Frolov I.V.²,
Postgrad. student Kuzmin N.P.¹, PhD Radaev O.A.²

¹Ulyanovsk State Technical University

²Ulyanovsk branch of the Kotelnikov Institute of Radioengineering and Electronics of RAS

The paper discusses the principles of designing wireless sensors with an optical method of data transmission intended for object monitoring systems and intelligent control systems. An analysis of modern wireless data transmission technologies used in sensor networks is carried out, and the limitations of conventional radio-frequency protocols associated with heavy spectrum congestion and electromagnetic compatibility issues are considered. The prospects of using optical communication channels to improve noise immunity and reliability of data transmission are demonstrated. Design approaches for wireless temperature sensors based on a Schmitt trigger integrated circuit and the specialized NST1001 microchip with an optical data transmission channel are proposed and described. Two methods for separating signals from spatially distributed sensors are presented: address-time multiplexing with data transmission at a single wavelength and spectral channel separation based on optical wavelength division using light-emitting diodes with different spectral ranges and photodetectors equipped with optical filters. A comparative analysis of the proposed signal separation methods is performed, and the features of their practical implementation are determined.



ДЕКОДИРОВАНИЕ ЛИНЕЙНЫХ ПОМЕХОУСТОЙЧИВЫХ КОДОВ С ИСПРАВЛЕНИЕМ СТИРАНИЙ ЗА ПРЕДЕЛАМИ МИНИМАЛЬНОГО КОДОВОГО РАССТОЯНИЯ

д.т.н., Квашенников В.В.
к.т.н., доц. Шабанов А.К.

АО «Калужский научно-исследовательский институт телемеханических устройств»

Рассмотрено декодирование линейных помехоустойчивых кодов с исправлением стираний. Декодирование с исправлением стираний сводится к решению системы линейных уравнений относительно значений стираний. Алгоритм декодирования исправляет все стирания в пределах минимального кодового расстояния кода и полностью реализует корректирующую способность за пределами минимального кодового расстояния. Помехоустойчивый код исправляет примерно вдвое большее число стираний, чем ошибок. Поэтому, помехоустойчивость кода при исправлении стираний не хуже, чем при исправлении ошибок, при условии достаточно высокой вероятности стирания ошибочных символов и небольшой вероятности стирания правильных символов. Декодирование является универсальным, применимым для любого линейного кода. Сложность декодирования двоичного кода оценивается полиномиальным законом с показателем степени не более 2. Приведен пример декодирования двоичного кода БЧХ (15,7,5) с исправлением 8 стираний, что на 4 стирания больше, чем при исправлении стираний в пределах минимального кодового расстояния.

В каналах связи с шумами широко применяют помехоустойчивое кодирование. Для декодирования кодов используют различные алгоритмы, из которых наибольшую помехоустойчивость обеспечивают алгоритмы мягкого декодирования кодов. Однако, многие алгоритмы мягкого декодирования имеют высокую сложность, что затрудняет их использование на практике, особенно для длинных кодов [1,2]. В данной работе описано декодирование кодов с исправлением стираний [3]. Сложность декодирования с исправлением стираний меньше сложности декодирования с исправлением ошибок, а помехоустойчивость не хуже. Высокая помехоустойчивость обеспечивается за счет вдвое большего числа корректируемых стираний, по сравнению с числом корректируемых ошибок. При этом алгоритм с исправлением стираний полностью реализует корректирующую способность за пределами минимального кодового расстояния [4].

Важным при декодировании с исправлением стираний является выбор критериев стирания недоверенных символов кода. Выделим три основных критерия стирания символов:

1. По амплитуде сигнала на выходе интегратора демодулятора менее заданной пороговой величины.
2. По числу ошибочных контрольных проверок символов с использованием слов дуального кода минимального веса.
3. По дополнительной контрольной сумме для проверки правильности декодирования кода.

Критерии стирания должны обеспечивать максимальную вероятность стирания ошибочных символов P_{os} и минимальную вероятность стирания правильных символов P_{ps} . При использовании 1-го критерия $P_{ps} \approx P_{os}$ [5,6]. Поэтому на практике чаще используют 2-ой или 3-ий критерии, с достаточно большой вероятностью стирания ошибочных символов и малой вероятностью стирания правильных символов. Однако, 3-ий критерий требует введения дополнительной избыточности, что снижает скорость передачи в канале связи.

Кодирование линейного помехоустойчивого кода над полем Галуа $GF(p^m)$

$$R=A \times G, \quad (1)$$

где G – порождающая матрица размера $k \times n$, A – вектор-строка исходной информации длины k символов, R – вектор-строка символов кода длины n , $k < n$.

Помехоустойчивый код гарантированно исправляет $s=d-1$ стираний. Код может также исправлять часть стираний за пределами минимального кодового расстояния $s \geq d$, вплоть до $s=n-k$. Оценки доли исправляемых кодом стираний за пределами минимального кодового расстояния приведены в [7,8].

Запишем принятое кодовое слово со стираниями

$$B=b_0b_{1..x_1}...b_{j..}x_{2..}b_{f..}x_{s..}b_{n-s-1},$$

где b_i – значение i -го принятого символа, x_i – неизвестное значение i -го стертых символа.

Система линейных уравнений для безошибочно принятых символов

$$B \times H^T = 0, \quad (2)$$

где H – проверочная матрица кода размера $(n-k) \times n$.

Запишем (2) в виде

$$X \times H_x^T = -B_x \times H_b^T, \quad (3)$$

В системе (3) вектор B разделяют на два блочных вектора, первый из которых включает неизвестные стирания, а второй – принятые символы кода. Матрицу H также разделяют на блочные матрицы, соответствующие стираниям и принятым символам кода. Из системы линейных уравнений определяют

неизвестные значения стираний $X=x_1x_2...x_s$, [9].

Решение системы выполняют одним из известных методов, например, методом Жордана-Гаусса [10,11]. При линейной независимости столбцов проверочной матрицы, соответствующих стираниям, система имеет единственное решение. Если число линейно независимых столбцов больше либо равно минимальному кодовому расстоянию, то определяют значения стираний за пределами минимального кодового расстояния. Для двоичных кодов вычисления используют только операции поразрядного сложения по модулю 2 и перестановки строк проверочной матрицы, и сложность оценивается $O(s^2)$.

Для декодирования кода с исправлением стираний необходимо обеспечить высокую вероятность стирания ошибочных символов кода и низкую вероятность стирания правильных символов. В данной работе рассмотрен 2-ой критерий стирания символов, использующий проверочные соотношения на основе слов дуального кода минимального веса. Согласно этого критерия, чем больше проверочных соотношений кода выполняются, тем больше будет достоверность символа. При этом критерий не требует введения дополнительной избыточности.

Слова дуального кода определяют через проверочную матрицу кода

$$D=A \times H,$$

где A – вектор-строка исходной информации длины $n-k$, H – проверочная матрица кода.

Поскольку

$$B \times D^T = 0,$$

то любое слово дуального кода задает проверочное соотношение кода.

Пусть d_0 – минимальное кодовое расстояние дуального кода. Выберем M слов дуального кода $D_1 D_2 \dots D_M$ веса d_0 . Из слов дуального кода минимального веса составим матрицу проверок размера $M \times n$, $M \geq (n-k)$

$$F = \begin{bmatrix} D_1 \\ D_2 \\ \dots \\ D_M \end{bmatrix}.$$

На кодовое слово может быть наложен вектор ошибок $B=A+E$, тогда вектор проверок $S=S_1 S_2 \dots S_M$
 $S=B \times F^T = E \times F^T$.

В общем случае вектор проверок отличается от вектора синдрома ошибок. Проверка выполняется $S_i=0$, если вектор E в окне минимального веса d_0 , задаваемом проверкой D_i , не содержит ошибок или содержит четное число ошибок. Проверка не выполняется $S_i=1$, если вектор E в окне проверки содержит нечетное число ошибок. При небольшом весе проверок d_0 число ошибок в проверке будет небольшим. Поэтому, проверки чаще выполняются при безошибочном приеме символов кода, а не выполняются – из-за одиночных ошибок. Для канала с независимыми ошибками вероятность t ошибок в проверке веса d_0

$$P(d_0, t) = C_{d_0}^t p^t (1-p)^{d_0-t},$$

где p – средняя вероятность ошибки на бит в канале связи.

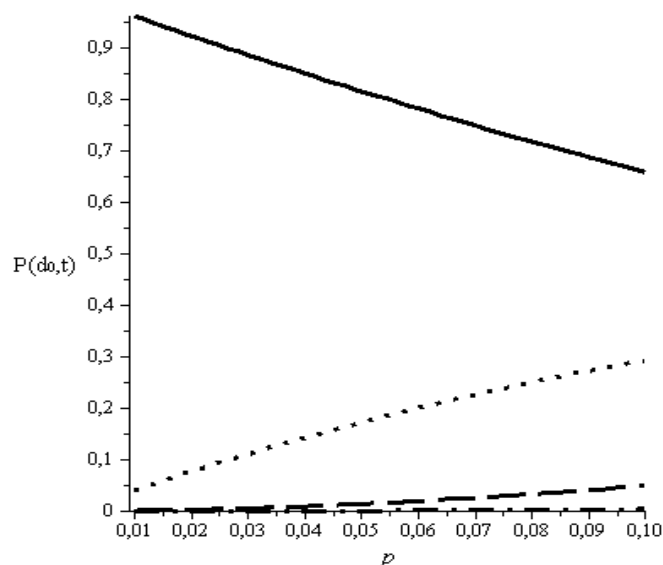


Рисунок 1 Вероятность t ошибок в проверке минимального веса от p .

На рисунке 1 представлены графики зависимости $P(d_0, t)$ от p для двоичного кода БЧХ(15,7,5), $n=15$, $k=7$,

$d = 5, d_0 = 4$. Верхняя кривая – $t=0$, зависимости, расположенные ниже, соответствуют $t=1,2,3$.

Вероятность безошибочных проверок больше вероятности проверок с одиночными ошибками запишется

$$(1-p)^{d_0} > d_0 p (1-p)^{d_0-1}.$$

$$\frac{1-p}{p} > d_0.$$

Если в канале $p < 0.03$, то $d_0 < 32$. На практике используют коды со значительно меньшим d_0 и последнее неравенство гарантированно выполняется. Поэтому, проверки $S=S_1 S_2 \dots S_M$ оценивают достоверности символов, входящих в проверки. Нулевые проверки повышают достоверность символа, а единичные – снижают достоверность символа. Устанавливая некоторое пороговое значение, стирают символы, число единичных проверок которых больше порогового значения.

Матрица проверок F линейного кода задает двудольный граф Таннера, одно множество узлов которого соответствует множеству проверок (проверочные узлы), другое – множеству кодовых символов (символьные узлы) [12]. На рисунке 2 представлен граф Таннера кода БЧХ(15,7,5), показывающий связи между 15 символами кода и 15 проверками минимального веса. Каждый символьный узел в графе связан ребрами с 4 проверочными узлами. В каждый проверочный узел входит 4 символа. При довольно большой средней вероятности ошибки на бит в канале $p=0,01$ вероятность безошибочных проверок веса 4 оценивается $P_0=0.9606$, вероятность проверок с одной ошибкой $P_1=0.0388$, двумя – $P_2=0.000588$ и т.д. Вероятность проверок с тремя и более ошибками ничтожно мала.



Рисунок 2 Граф Таннера проверок минимального веса кода БЧХ(15,7,5)

Из 15 проверок минимального веса 4 в среднем более 14 проверок будут безошибочными, менее 1 – с одной ошибкой, близко к 0 – с двумя ошибками. В среднем 14 проверок будут выполняться и 1 проверка выполняться не будет. Соотношение между числом выполняемых проверок и числом невыполняемых проверок 14:1. Достоверность символа определяется по весу вектора проверок данного символа.

Рассмотрим пример декодирования двоичного кода БЧХ(15,7,5) с исправлением стираний. Стирания веса $s=4$ и менее гарантированно исправляются, доля исправляемых стираний веса 5 равна 0,9964, 6 - 0,9702, 7 - 0,8597, 8 - 0,5061. Порождающая и проверочная матрицы кода

$$G = \begin{pmatrix} 001010100101100 \\ 101000111111011 \\ 000110111110011 \\ 100101000011101 \\ 011001010000111 \\ 001011000010101 \\ 010100101100001 \end{pmatrix}, \quad H = \begin{pmatrix} 110001001101011 \\ 101011110001001 \\ 100110101111000 \\ 100011000110001 \\ 100100010110100 \\ 001010010100101 \\ 111100100111000 \\ 100010011010111 \end{pmatrix}.$$

Пусть передавался код $R=100110101111000$, а принят код $B=110010001101001$ с достоверностями

символов $\alpha=0.9, 0.3, 0.8, 0.3, 0.4, 0.8, 0.3, 0.7, 0.9, 0.5, 0.3, 0.8, 0.4, 0.7, 0.2$.

Символы кода на $i=13, 11, 10, 8, 5, 4, 2, 0$ позициях кода с достоверностями $\leq 0,5$ стираем

$$B=1x_{13}0x_{11}x_{10}0x_801x_5x_41x_20x_0.$$

Всего стерто 8 символов.

Система 8 линейных уравнений с коэффициентами из $13, 11, 10, 8, 5, 4, 2, 0$ столбцов проверочной матрицы не имеет решения. Выбираем наиболее достоверный символ среди недостоверных символов. Это будет символ x_5 с достоверностью, равной 0,5. Система 7 линейных уравнений с коэффициентами из $13, 11, 10, 8, 4, 2, 0$ столбцов проверочной матрицы имеет единственное решение.

По методу Жордана-Гаусса ортогональные проверки для стираний

$$H_1 = \begin{vmatrix} 111001010100000 \\ 000101011101010 \\ 100011011100000 \\ 000000110100010 \\ 000000011010000 \\ 100001010001110 \\ 001000011001011 \end{vmatrix}$$

Ортогональные проверки содержат только одну 1 в столбце, соответствующем стиранию, что позволяет выразить это стирание через принятые символы кода.

При $a_5=0$ – первое решение

$$\begin{aligned} a_0 &= a_{12} + a_7 + a_6 + a_3 + a_1 = 0 \\ a_2 &= a_{14} + a_9 + a_7 + a_3 + a_1 = 0 \\ a_4 &= a_7 + a_6 = 1 \\ a_8 &= a_7 + a_5 + a_1 = 0 \\ a_{10} &= a_{14} + a_9 + a_7 + a_6 + a_5 = 0 \\ a_{11} &= a_9 + a_7 + a_6 + a_5 + a_3 + a_1 = 0 \\ a_{13} &= a_{14} + a_{12} + a_9 + a_7 + a_5 = 1 \end{aligned}$$

При $a_5=1$ – второе решение

$$\begin{aligned} a_0 &= a_{12} + a_7 + a_6 + a_3 + a_1 = 0 \\ a_2 &= a_{14} + a_9 + a_7 + a_3 + a_1 = 0 \\ a_4 &= a_7 + a_6 = 1 \\ a_8 &= a_7 + a_5 + a_1 = 1 \\ a_{10} &= a_{14} + a_9 + a_7 + a_6 + a_5 = 1 \\ a_{11} &= a_9 + a_7 + a_6 + a_5 + a_3 + a_1 = 1 \\ a_{13} &= a_{14} + a_{12} + a_9 + a_7 + a_5 = 0 \end{aligned}$$

С учетом достоверностей символов кода принимаем второе решение $B=100110101111000$, что совпадает с переданным кодовым словом.

Таким образом, исправлено 8 стираний символов кода БЧХ(15,7,5), что на 4 стирания больше, чем число исправляемых стираний в пределах минимального кодового расстояния.

Заключение. Алгоритм декодирования линейных помехоустойчивых кодов с исправлением стираний позволяет корректировать стирания за пределами минимального кодового расстояния. При этом сложность декодирования с исправлением стираний значительно меньше, чем сложность с декодирования с исправлением ошибок. Декодирование с исправлением стираний позволяет определять значения стираний при линейной независимости столбцов проверочной матрицы, соответствующих стираниям. Исправляют все стирания в пределах минимального кодового расстояния $s=d-1$ и часть стираний за пределами минимального

кодированного расстояния $n-k \geq s \geq d$. Для двоичных линейных кодов сложность декодирования оценивается $O(s^2)$. Помехоустойчивость декодирования с исправлением стираний обеспечивается при условии высокой вероятности стирания ошибочных символов и небольшой вероятности стирания правильных символов. Для стирания недостоверных символов используют контрольные проверки символов кода, задаваемые словами дуального кода минимального веса. Декодирования с исправлением стираний может применяться для любых линейных помехоустойчивых кодов.

Литература

1. Кларк Дж., мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. / Под ред. Б.С. Цыбакова // М.: Радио и связь. 1987. 392 с.
2. Moon T. K. Error Correction Coding. Mathematical Methods and Algorithms. / Hoboken. NJ. USA : Wiley. 2005. 320 p.
3. Бородин Л.Ф. Введение в теорию помехоустойчивого кодирования. / Л.Ф. Бородин. М.: Сов. Радио. 1968. 408 с.
4. Квашенников В.В. Способ декодирования линейных помехоустойчивых кодов с исправлением стираний. Патент на изобретение 2746797 С1, 21.04.2021. Заявка № 2020136340 от 03.11.2020.
5. Коричнев Л.П., Королев В.Д. Статистический контроль каналов связи. / М.: Радио и связь. 1989. 240 с.
6. Шувалов В.В. Прием сигналов с оценкой их качества. / М.: Связь. 1979. 223 с.
7. Попов О.В. Об оценке способности линейных кодов исправлять стирания и обнаруживать ошибки при наличии стираний. // Электросвязь. 1967. №10. с. 43-47.
8. Афанасьев В.Б., Давыдов А.А., Зигангиров Д.К. Оценка доли стираний, исправляемых линейными кодами. // Информационные процессы. 2016. т. 16. №4. с.382-404.
9. Колесник В.Д., МIRONЧИКОВ Е.Т. Декодирование циклических кодов. / М.: Связь. 1968. 251 с.
10. Гантмахер Ф.Р. Теория матриц. – М.: Наука. 1966. 576 с.
11. Ланкастер П. Теория матриц. – М.: Наука. 1973. 280 с.
12. Кудряшов Б. Д. Основы теории кодирования. – СПб.: БХВ-Петербург, 2016. 400 с

DECODING OF LINEAR NOISE-RESISTANT CODES WITH CORRECTION OF ERASURES BEYOND THE MINIMUM CODE DISTANCE

Dr. of Engineering, Kvashennikov V.V.
Ph.D., Associate Professor Shabanov A.K.

JSC Kaluga Research Institute of Telemechanic Devices, Kaluga

The decoding of linear error-correcting codes with erasure correction is considered. Erasure correction decoding reduces to solving a system of linear equations with respect to the erasure values. The decoding algorithm corrects all erasures within the minimum code distance of the code and fully realizes the correcting ability beyond the minimum code distance. The error-correcting code corrects approximately twice as many erasures as errors. Therefore, the noise immunity of the code in the case of erasure correction is not worse than in the case of error correction, provided that the probability of erasing erroneous symbols is sufficiently high and the probability of erasing correct symbols is low. Decoding is universal and can be applied to any linear code. The complexity of decoding a binary code is estimated by a polynomial law with a degree of at most 2. An example of decoding a binary BCH code (15,7,5) with 8 erasures corrected is given, which is 4 erasures more than when erasures are corrected within the minimum code distance.



УНКЦИЯ ПОТЕРЬ ДЛЯ РОБАСТНОЙ АДАПТИВНОЙ ОБРАБОТКИ РАДИОСИГНАЛОВ НА ОСНОВЕ L1 И L2 НОРМ

к.т.н. Мокринский Д.В., д.т.н. Тоискин В.Е.

Филиал Военной академии Ракетных войск Стратегического назначения им. Петра Великого

В работе предлагается подход к робастной адаптивной фильтрации сигналов в условиях сложной импульсной помеховой обстановки, основанный на использовании комбинированных функций потерь. Предложенный метод использует линейную комбинацию функций влияния, базирующихся на L1 и L2 нормах, что позволяет гибко адаптироваться к различным видам помех без существенного увеличения вычислительной сложности. Представлена математическая модель комбинированной функции потерь и показано, что варьирование весовых коэффициентов позволяет эффективно подстраиваться под изменяющуюся помеховую обстановку. Показано, что комбинированные функции потерь особенно эффективны для декаметровых (ДКМВ) каналов связи, характеризующихся одновременным воздействием интенсивных редких импульсных помех и слабых частых помех. Предложенный метод может быть реализован как с фиксированными, так и с адаптивными весовыми коэффициентами.

1. Введение

Адаптивная фильтрация является фундаментальной задачей цифровой обработки сигналов и находит широкое применение в системах связи, радиолокации, акустической обработки и других областях [1]. Классические алгоритмы адаптивной фильтрации, такие как метод наименьших средних квадратов (Least Mean Squares, LMS) и рекурсивный метод наименьших квадратов (Recursive Least Squares, RLS), оптимизируют среднеквадратичную ошибку и демонстрируют высокую эффективность в условиях гауссовских помех [1-2].

Однако в реальных каналах связи, например в декаметровом (ДКМВ) диапазоне, помеховая обстановка характеризуется присутствием импульсных помех с негауссовским распределением [3-4]. Такие помехи приводят к значительной деградации характеристик стандартных адаптивных алгоритмов, основанных на минимизации среднеквадратичной ошибки. Для решения данной проблемы разработаны робастные методы адаптивной фильтрации, использующие М-оценки и соответствующие функции влияния [5].

Основная идея робастного подхода заключается в замене квадратичной функции потерь на нелинейную функцию, ограничивающую влияние выбросов. Функция влияния определяет степень воздействия каждого отсчета ошибки на обновление весовых коэффициентов адаптивного фильтра [8]. Классические робастные функции влияния, такие как функция Хубера (Huber), Хэмпела (Hampel), Тьюки (Tukey), обеспечивают компромисс между эффективностью в гауссовской среде и робастностью к выбросам [5-6].

Рассмотрим задачу адаптивной коррекции радиоканала. Сигнал с выхода адаптивного эквалайзера в момент времени n формируется как

$$y(n) = \mathbf{w}^H \mathbf{x}(n) + v(n), \quad (1)$$

где $\mathbf{w} \in \mathbb{C}^M$ – текущий вектор весовых коэффициентов цифрового фильтра; $\mathbf{x} \in \mathbb{C}^M$ – вектор входных отсчетов, $v(n)$ – аддитивная помеха, M – порядок фильтра.

Ошибка фильтрации (апостериорная ошибка) вычисляется как

$$e(n) = d(n) - y(n), \quad (2)$$

где $d(n)$ – значения отсчетов обучающей последовательности адаптивного эквалайзера.

Алгоритм LMS основан на минимизации мгновенного среднеквадратического значения ошибки и имеет следующий вид рекуррентного соотношения:

$$\mathbf{w}(n+1) = \mathbf{w}(n) + \mu \mathbf{x}(n) e(n), \quad (3)$$

где μ – параметр размера шага, определяющий скорость адаптации и устойчивость алгоритма.

Алгоритм RLS минимизирует взвешенную сумму квадратов ошибок от начала процесса адаптации до текущего момента времени:

$$J(\mathbf{w}) = \sum_{i=1}^n \lambda^{n-i} e^2(i), \quad (4)$$

где $\lambda \in (0, 1]$ – фактор забывания.

Рекуррентные соотношения для алгоритма RLS имеют вид:

$$\begin{aligned} \mathbf{k}(n) &= \frac{\lambda^{-1} \mathbf{P}(n-1) \mathbf{x}(n)}{1 + \lambda^{-1} \mathbf{x}^H(n) \mathbf{P}(n-1) \mathbf{x}(n)}, \\ e(n) &= d(n) - \mathbf{w}^T(n-1) \mathbf{x}(n), \\ \mathbf{w}(n) &= \mathbf{w}(n-1) + \mathbf{k}(n) e(n), \end{aligned} \quad (5)$$

$$\mathbf{P}(n) = \lambda^{-1} \mathbf{P}(n-1) - \lambda^{-1} \mathbf{k}(n) \mathbf{x}^H(n) \mathbf{P}(n-1),$$

где $\mathbf{k}(n)$ – вектор коэффициентов усиления, $\mathbf{P}(n)$ – матрица обратной корреляции входных данных, λ – фактор забывания [1-2].

Робастный алгоритм адаптации получается заменой ошибки $e(n)$ на значение функции влияния $\psi(e(n))$. Для алгоритма типа LMS робастный вариант имеет вид:

$$\mathbf{w}(n+1) = \mathbf{w}(n) + \mu \mathbf{x}(n) \psi(e(n)), \quad (6)$$

а для алгоритма типа RLS (M-RLS):

$$\mathbf{w}(n+1) = \mathbf{w}(n) + \mathbf{k}(n) \psi(e(n)). \quad (7)$$

Функция влияния $\psi(e)$ ограничивает вклад больших значений ошибки в процесс адаптации, обеспечивая робастность алгоритма [7,8].

Современные исследования показывают, что комбинирование различных функций потерь может обеспечить лучшую адаптацию к изменяющимся условиям помеховой обстановки [9,10]. Настоящая статья предлагает систематический подход к использованию комбинированных функций потерь на примере функций, основанных на L1 и L2 нормах для робастной адаптивной обработки радиосигналов в каналах со сложной помеховой обстановкой.

2. Комбинированная функция влияния на основе L1 и L2 – норм

Рассмотрим простейший случай комбинации двух функций влияния, основанных на L2 и L1 нормах. Функция влияния на основе L2-нормы (квадратичная функция потерь):

$$\psi_{L2}(e) = e, \quad (8)$$

$$\rho_{L2}(e) = \frac{1}{2} e^2, \quad (9)$$

Функция влияния на основе L1-нормы:

$$\psi_{L1}(e) = \text{sign}(e) = \begin{cases} 1, & e > 0, \\ 0, & e = 0, \\ -1, & e < 0, \end{cases} \quad (10)$$

$$\rho_{L1}(e) = |e|, \quad (11)$$

Комбинированная функция влияния определяется как:

$$\psi_{L1L2}(e, a) = a |e| + \frac{1-a}{2} e^2, \quad (12)$$

Таким образом получаем следующие итерационные уравнения для обновления вектора весовых коэффициентов:

для LMS:

$$\mathbf{w}(n+1) = \mathbf{w}(n) + \mu \mathbf{x}(n) \left(a |e| + \frac{1-a}{2} e^2 \right), \quad (13)$$

для RLS:

$$\mathbf{w}(n+1) = \mathbf{w}(n) + \mathbf{k}(n) \left(a |e| + \frac{1-a}{2} e^2 \right). \quad (14)$$

Параметр a определяет баланс между робастностью к выбросам (L1-компонента) и эффективностью в гауссовской среде (L2-компонента):

$a = 0$ - квадратичная функция потерь (классический LMS/RLS): оптимальна для гауссовских помех, чувствительна к выбросам.

$a = 1$ - функция потерь на основе абсолютного значения (Least Absolute Deviation, LAD): максимальная робастность к выбросам, но медленная сходимость в отсутствие помех.

$0 < \alpha < 1$ - гибридная функция, обеспечивающая компромисс между скоростью сходимости и робастностью.

Оптимальное значение параметра α зависит от характеристик импульсных помех, в частности, от вероятности появления импульсов P_{imp} и отношения интенсивности импульсной помехи к фоновому шуму.

3. Моделирование процесса адаптации

Для демонстрации эффективности предложенного метода проведено численное моделирование.

Модель помехи $v(n)$ представляется в виде:

$$v(n) = v_0(n) + \sum_{i=1}^{N_{imp}} b_i(n) \xi_i(n), \quad (15)$$

где $v_0(n)$ – фоновый гауссовский шум с нулевым средним и дисперсией σ_0^2 , $b_i(n)$ – бернуллиевская случайная величина ($b_i(n) = 1$ с вероятностью p_i), $\xi_i(n)$ – импульсная помеха с амплитудой A_i и случайным знаком, N_{imp} – количество типов импульсных помех.

Параметры моделирования: частота дискретизации $F_s=2400$ (Гц); символьная скорость 2400 бод; количество символов для передачи 20000; ОСШ – 10 дБ. Тип модуляции – QPSK. Параметры канала связи: двухлучевой канал, задержка между лучами 2.2×10^{-3} с. Ослабление луча относительно основного: первый вариант – 100 дБ, второй – 5 дБ; доплеровское расширение: первый вариант – 0.1 Гц, второй – 1 Гц. Есть возможность задать воздействие двумя импульсными помехами с амплитудами A_1 и A_2 и вероятностями возникновения p_1, p_2 .

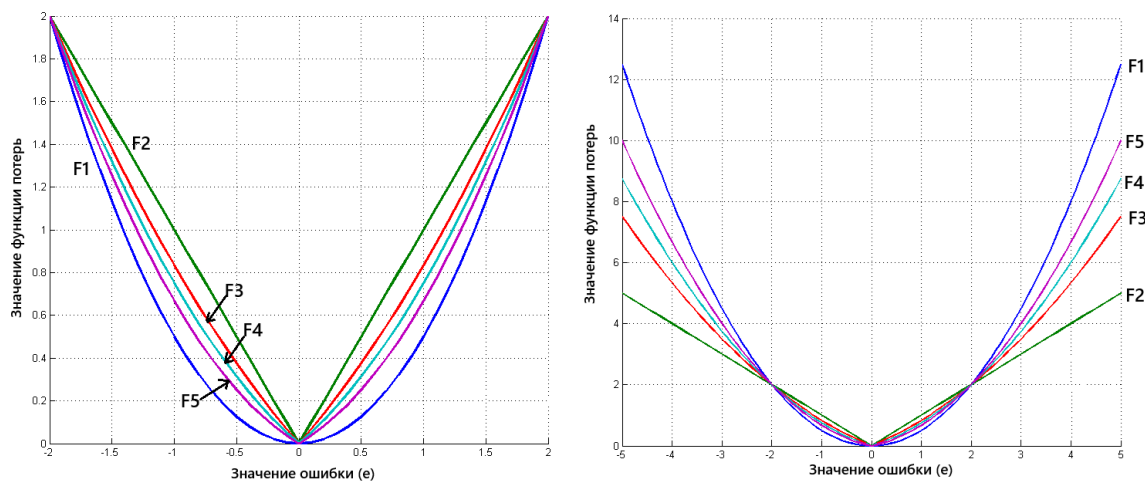


Рисунок 1. Используемые функции потерь.

Используются адаптивные эквалайзеры без обратной связи по решению с алгоритмами LMS и RLS. Порядок используемых фильтров: 8. Шаг LMS алгоритма: $\mu = 0.01$; фактор забывания для RLS $\lambda = 0.99$, реализован режим непрерывного обучения.

Используются следующие функции влияния (рисунок 1):

F1 – квадратичная функция ошибки на основе L2 – нормы;

F2 – робастная функция ошибки на основе L1 – нормы;

F3 – комбинированная функция: $0.35 \psi_{L1} + 0.65 \psi_{L2}$;

F4 – комбинированная функция: $0.5 \psi_{L1} + 0.5 \psi_{L2}$;

F5 – комбинированная функция: $0.65 \psi_{L1} + 0.35 \psi_{L2}$.

Результаты моделирования представлены в таблицах 1-3, рисунки 2-4 в качестве критерия эффективности используется вероятность битовой ошибки (BER) после детектирования.

Таблица 1.

Результаты моделирования для RLS алгоритма

1 помеха		2 помеха		RLS				
p_1	A_1	p_2	A_2	F1	F2	F3	F4	F5
L1/L2 (первый вариант)								
-	-	-	-	0,0408	0,0464	0,0433	0,042	0,0412
0,05	3	-	-	0,07	0,068	0,0668	0,067	0,0667
0,01	20	-	-	0,108	0,0537	0,0654	0,074	0,081
0,15	2	0,01	4	0,1066	0,1039	0,103	0,1036	0,105
L1/L2 (второй вариант)								
-	-	-	-	0,0776	0,0838	0,0797	0,0785	0,078
0,01	20	-	-	0,1739	0,1207	0,1382	0,146	0,161
0,05	3	-	-	0,1376	0,1387	0,1354	0,1349	0,1343
0,01	2	0,01	4	0,1188	0,1158	0,1145	0,1151	0,116
0,05	2,5	0,0025	8	0,146	0,1476	0,1428	0,1427	0,143

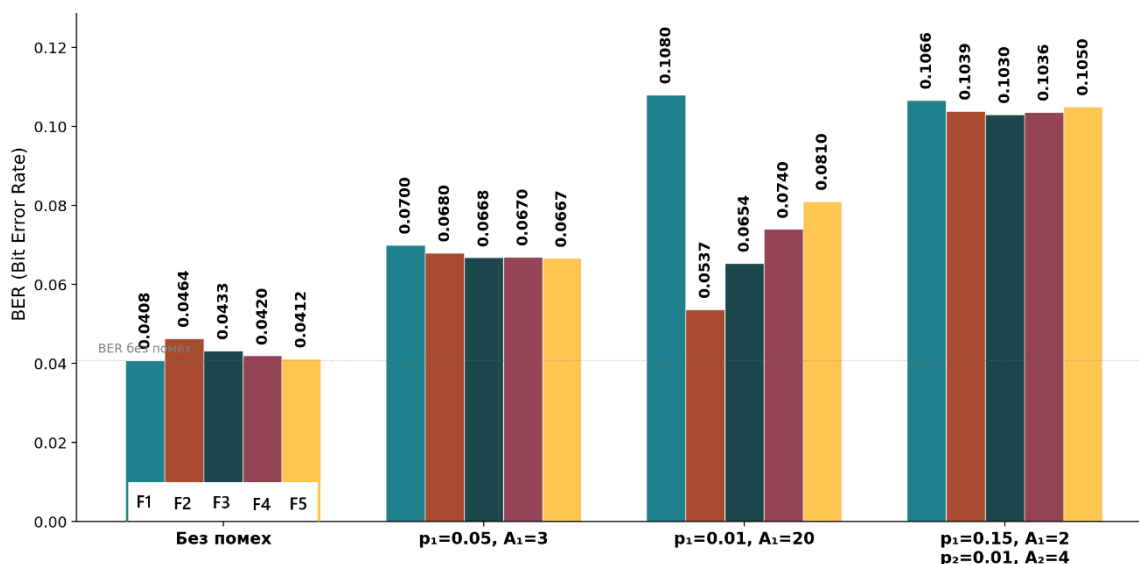


Рисунок 2. Результаты моделирования для RLS алгоритма (первый вариант)

4. Анализ результатов моделирования

По результатам анализа видно, что чувствительность к энергии помех монотонно возрастает с увеличением доли L2-компоненты в комбинации. В отсутствие помех квадратичная функция ($\alpha=0$) оптимальна, добавление L1-компоненты монотонно ухудшает характеристики; при слабых помехах добавление L1-компоненты улучшает робастность; при интенсивных выбросах L1-норма обеспечивает наилучший результат.

В таблице 3 приведена корреляция между эффективностью функций в различных условиях для RLS алгоритма.

Из таблицы 3 видно, что наибольшая отрицательная корреляция между F1 и F2 что подтверждает их противоположную направленность. Комбинированные функции F3-F5 имеют наиболее выраженную корреляционную связь друг с другом.

Сравнительный анализ RLS и LMS алгоритмов между собой показывает, что в отсутствие помех RLS незначительно (4-7%) превосходит LMS, однако при интенсивных помехах преимущество RLS достигает 48-78%. Комбинированные функции в RLS обеспечивают более плавное изменение характеристик при вариации параметров помех.

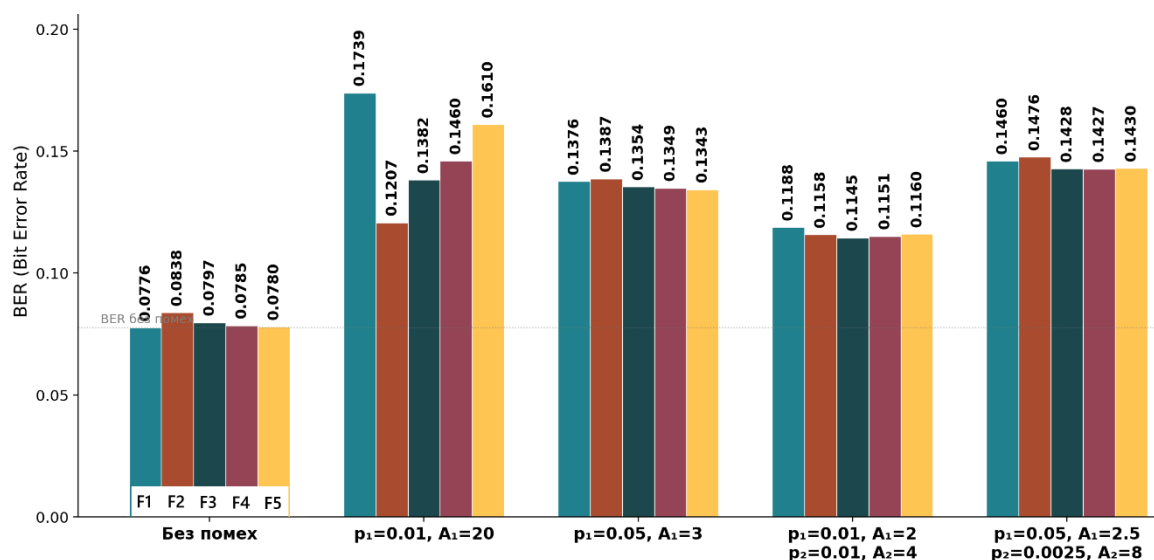


Рисунок 3. Результаты моделирования для RLS алгоритма (второй вариант)

Таблица 2.

Результаты моделирования для LMS алгоритма

1 помеха		2 помеха		LMS				
p_1	A_1	p_2	A_2	F1	F2	F3	F4	F5
L1/L2 (первый вариант)								
-	-	-	-	0,0426	0,0498	0,0457	0,0437	0,0439
0,05	3	-	-	0,0755	0,0767	0,0754	0,0759	0,0763
0,01	20	-	-	0,4889	0,1024	0,2785	0,3463	0,38
0,15	2	0,01	4	0,1277	0,1229	0,1199	0,1209	0,124

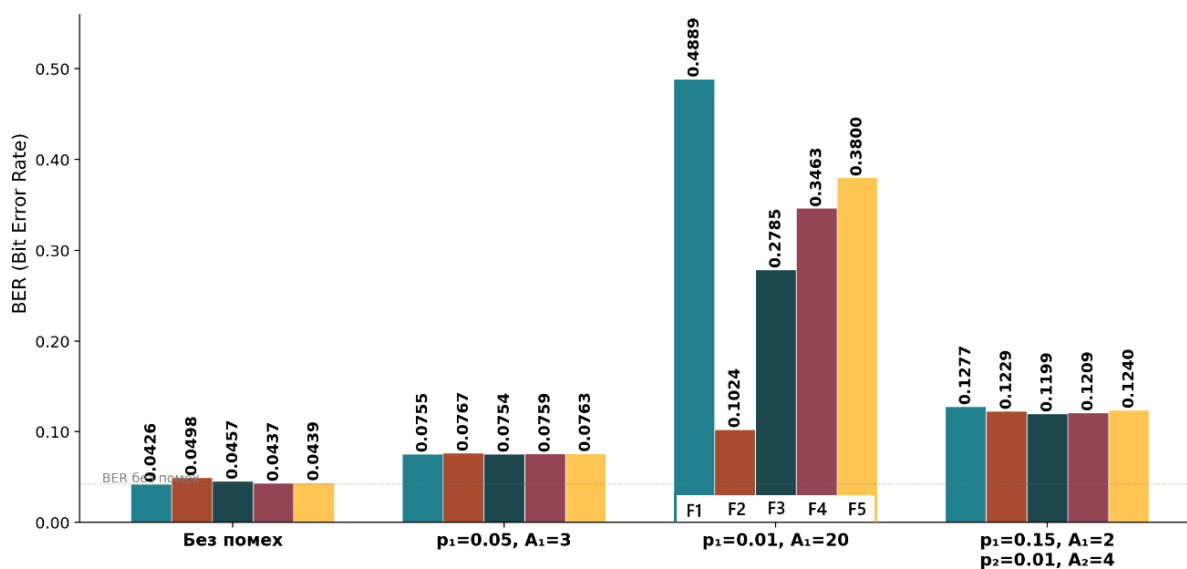


Рисунок 4. Результаты моделирования для LMS алгоритма

Таблица 3.

Корреляция между эффективностью функций влияния

	F1	F2	F3	F4	F5
F1	1	-0,32	0,86	0,91	0,94
F2	-0,32	1	0,15	-0,08	-0,21
F3	0,86	0,15	1	0,97	0,96
F4	0,91	-0,08	0,97	1	0,99
F5	0,94	-0,21	0,96	0,99	1

На основе анализа результатов моделирования определены оптимальные диапазоны α для различных типов помеховой обстановки:

Таблица 4

Оптимальные диапазоны для различной помеховой обстановки

Тип помеховой обстановки	Характеристики	Оптимальный α	Рекомендуемая функция
Чистый канал	Отсутствие помех	0,0-0,1	F1
Слабые гауссоподобные помехи	$A < 3, p$ любая	0,1-0,3	F3
Частые помехи средней интенсивности	$3 < A < 10, p > 0,05$	0,3-0,5	F3-F4
Смешанные помехи	Комбинация типов	0,4-0,6	F4
Интенсивные редкие выбросы	$A > 15, p < 0,02$	0,6-0,8	F4-F5
Экстремальные выбросы	$A > 50, p < 0,01$	0,8-1,0	F5-F2

В 60% исследованных сценариев комбинированные функции (F3-F5) показали результаты не хуже 5% от оптимальной специализированной функции; в 40% сценариев со смешанными помехами комбинированные функции превосходили обе базовые функции. Для практических приложений рекомендуется адаптивная подстройка α в диапазоне 0,3-0,7. Для систем с фиксированной функцией потерь оптимален выбор $\alpha = 0,5$ (F4), обеспечивающий наилучший компромисс. Для адаптивных систем целесообразно реализовать двухконтурную схему с подстройкой α на основе оценки эксцесса ошибки или отношения сигнал/помеха.

5. Заключение

В настоящей работе предложен и исследован метод робастной адаптивной фильтрации на основе комбинированных функций потерь, использующих линейную комбинацию функций влияния, базирующихся на L1 и L2 нормах.

Показано, что варьирование весовых коэффициентов линейной комбинации позволяет гибко адаптироваться к различным типам помеховой обстановки без увеличения порядка фильтра и существенного роста вычислительной сложности.

На примере простейшей комбинации L1 и L2 норм установлено соответствие между оптимальным значением весового коэффициента α и характеристиками импульсных помех (вероятность появления и интенсивность).

Предложенный метод потенциально эффективен для каналов ДКМВ связи, характеризующихся сложной помеховой обстановкой с одновременным присутствием нескольких типов импульсных помех различной интенсивности и частоты появления. При этом практическая реализация может осуществляться в двух режимах:

режим с переключением - дискретное изменение весовых коэффициентов α_k в зависимости от детектированного типа помеховой обстановки, что обеспечивает простоту реализации и низкие вычислительные затраты.

адаптивный режим [11] - непрерывная подстройка весовых коэффициентов на основе текущих статистических оценок помеховой обстановки в рамках двухконтурной схемы адаптации, что обеспечивает максимальную гибкость при умеренном увеличении вычислительной сложности.

Литература

1. Widrow, B., & Stearns, S. D. (1985). Adaptive Signal Processing. Prentice-Hall.
2. Джиган, В. И. Адаптивные фильтры: от теории до практики / В. И. Джиган // РЭУС-ИТ 2024 – Москва: Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова, 2024. – С. 9-12.
3. NTIA Report 91-277 Wideband HF Noise/Interference Modeling Part I: First-Order Statistics. 1991. – 124 p.
4. ITU-R Bandwidths, signal-to-noise ratios and fading allowances in HF fixed and land mobile radiocommunication systems. ITU-R Recommendation, 2015. – 24 p.
5. Zou, Y., Chan, S. C., & Ng, T. S. (2001). Robust M-estimate adaptive filtering. IEE Proceedings - Vision, Image and Signal Processing, 148(4), 289-294. <https://doi.org/10.1049/ip-vis:20010316>
6. Симахин В. А., Черепанов О. С., Шаманаева Л. Г. Обработка экспериментальных данных в условиях априорной статистической неопределенности. – Томск: Изд-во НТЛ, 2021. – 340 с.
7. Huber, P. J., & Ronchetti, E. M. (2009). Robust Statistics (2nd ed.). Wiley.
8. Hampel, F. R., Ronchetti, E. M., Rousseeuw, P. J., & Stahel, W. A. (1986). Robust Statistics: The Approach Based on Influence Functions. Wiley.
9. Maronna, R. A., Martin, R. D., Yohai, V. J., & Salibián-Barrera, M. (2019). Robust Statistics: Theory and Methods (2nd ed.). Wiley.
10. Chen, B., Xing, L., Zhao, H., Zheng, N., & Príncipe, J. C. (2021). Diffusion adaptive filtering algorithm based on the Fair cost function. Scientific Reports, 11, 20085. <https://doi.org/10.1038/s41598-021-99330-9>
11. Цимбал В. А., Мокринский Д. В., Тоискин В. Е. Проблема выбора неквадратичной рабочей функции для робастного алгоритма адаптивной фильтрации радиосигнала. // Телекоммуникация и связь, 2025, № 6 (09). С. 3-13.

LOSS FUNCTION FOR ROBUST ADAPTIVE RADIO SIGNAL PROCESSING BASED ON L1 AND L2 NORMS

Cand. Sci. (Tech.) D.V. Mokrinskiy, Dr. Sci. (Tech.) V.E. Toiskin

Branch of the Military Academy of Strategic Missile Forces named after Peter the Great (Serpukhov, Moscow Region)

This paper proposes an approach to robust adaptive signal filtering under complex impulsive interference conditions, employing combined loss functions. The proposed method utilizes a linear combination of influence functions based on the L1 and L2 norms, enabling flexible adaptation to various interference types without a substantial increase in computational complexity. A mathematical formulation of the combined loss function is presented, demonstrating that variation of the weighting coefficients allows effective tuning to time-varying interference environments. It is shown that combined loss functions are particularly efficient for decameter waveband communication channels, which are characterized by the simultaneous presence of intense, rare impulsive disturbances and weak frequent noise.



ПОВЫШЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ ПЕРСПЕКТИВНОЙ ПАКЕТНОЙ СЕТИ РАДИОСВЯЗИ НА ОСНОВЕ МЕТОДА ФУНКЦИОНАЛЬНОГО СЖАТИЯ И МНОГОМЕРНОЙ МАРШРУТИЗАЦИИ ПАКЕТОВ

доц., к.т.н., Орехов С. Е., студ. Деменский Д. С.

Филиал Военной академии ракетных войск стратегического назначения имени Петра Великого

В статье рассмотрены основные пути повышения пропускной способности перспективной пакетной сети радиосвязи, среди которых обоснованно выделено направление, ориентированное на эффективное сжатие передаваемых по каналам связи данных. Изложен принцип и содержание нового метода функционального сжатия двоичной информации, позволяющего повысить пропускную способность перспективной пакетной сети радиосвязи за счет сжатия статистически выравненных данных. Кроме того, приведены предложения по реализации алгоритма функционального сжатия двоичной информации в рамках концептуальной схемы построения параллельного сетевого тракта в сети связи с многомерной маршрутизацией пакетов, что существенно повышает пропускную способность перспективной пакетной сети радиосвязи при рациональном использовании имеющихся аппаратно-программных ресурсов.

[1]

Под интегрированной системой управления [1, 2] понимается такая система управления, в которую встроены программные интерфейсы взаимодействия с обеспечивающей ее автоматизированной системой связи. Отличительной особенностью интегрированных систем управления является совместное использование общей универсальной аппаратно-программной платформы, которая динамически реконфигурируется под требования той или иной системы. Реконфигурация платформы должна обеспечивать высокие показатели функциональной устойчивости и эффективности решения клиентских запросов [2].

Вместе с тем, особенностью перспективной интегрированной системы управления специального назначения является преимущественное использование радиоканалов метрового и дециметрового диапазонов пакетной сети радиосвязи в условиях сложной помеховой обстановки при достижении высокой разведзащищенности. Таким образом, повышение пропускной способности рассматриваемой системы управления становится возможным, как правило, за счет совершенствования алгоритмов сжатия информации, помехозащиты, маршрутизации и управления потоками, а также их программно-аппаратного обеспечения [3-5].

В статье рассматривается метод функционального сжатия двоичной информации, позволяющий повысить пропускную способность перспективной пакетной сети радиосвязи за счет эффективного сжатия статистически выравненных данных, т.е. тех, которые подвергались криптографическому или статистическому кодированию [6, 7].

Сущность метода заключается в следующем.

Исходный блок двоичной информации I (BUBD – block of uncompressed binary data) сегментируется на множество субблоков $\{I_s\}$ определенных размеров согласно (1):

$$size(I_s) = n \times n \times k, \quad (1)$$

где $n \times n$ – размер кодовой таблицы (CTS – coding table size);

k – разрядность символа CTS a_{ij}^* .

Символ CTS дополняется последовательностью служебных разрядов **nonce1**, в которой старший разряд **sign1** определяет знак расширенного символа a_{ij} . Формат расширенного символа представлен выражением (2).

$$a_{ij} = \left[\begin{array}{c} \text{sign1} \\ \hline \text{nonce1} \end{array} \right] \left[a_{ij}^* \right] \quad (2)$$

Расширенные символы, в свою очередь, являются элементами матрицы коэффициентов A СЛАУ размером $n \times n$ [8]. Формат элементов вектора свободных членов (B), вынесенных в правую часть уравнений, соответствует выражению (3) и представляет собой только последовательность служебных разрядов **nonce2**, в которой старший разряд **sign2** определяет знак свободного члена b_i .

$$b_i = \left[\begin{array}{c} \text{sign2} \\ \hline \text{nonce2} \end{array} \right] \quad (3)$$

Для полноценной работы алгоритма сжатия необходимо вычислить значение хеш-функции h матрицы коэффициентов A СЛАУ любым из известных способов [8].

$$h = hash(A) \quad (4)$$

Очевидно, что вариантов решения такой СЛАУ (X) большое множество [8], однако выбирается тот, который при последовательном переборе комбинаций *nonce1* и *nonce2* позволяет однозначно определить искомую матрицу A по значению ее хеш-функции при первом же совпадении.

Упрощенная схема процесса функционального сжатия блока двоичных данных представлена на рисунке 1.

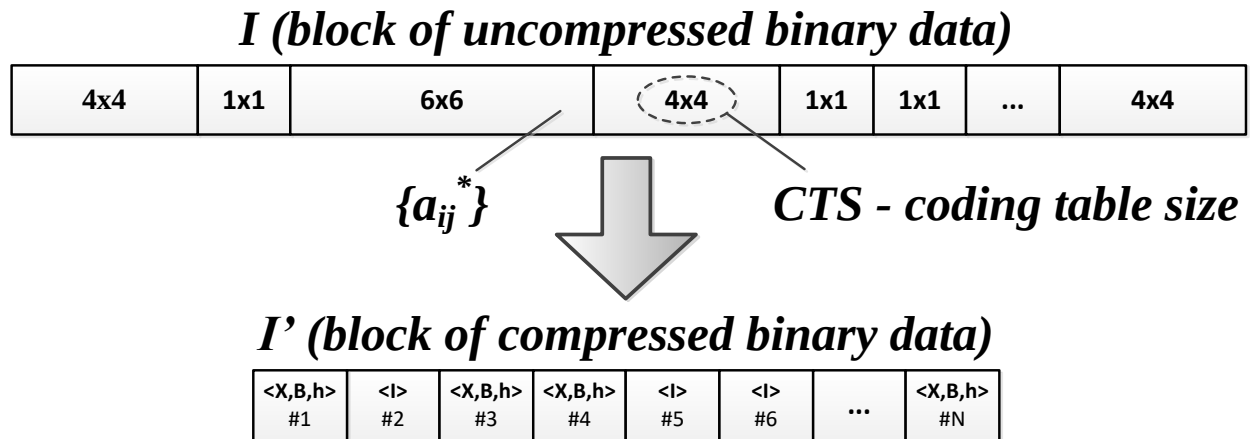


Рисунок 1 – Упрощенная схема процесса функционального сжатия блока двоичных данных

На рисунке CTS 1×1 обозначает субблок, не подвергнутый компрессии, т.е. передающийся по каналу связи без сжатия. Следует отметить, что, как показали исследования, сжатие становится возможным при $n > 3$, поэтому остальные субблоки со значениями CTS 4×4 и более прошли процедуру компрессии.

В отличие от существующих методов сжатия информации без потерь, таких как [6]:

- 1) разделение мантисс и экспонент;
- 2) канонический метод Хаффмана;
- 3) арифметическое сжатие;
- 4) нумерующее кодирование;
- 5) скалярное и векторное квантование;
- 6) словарные методы сжатия данных;
- 7) методы контекстного моделирования;
- 8) сортировка параллельных блоков;
- 9) фрагментирование;
- 10) препроцессинг

Функциональное сжатие не оперирует способами устранения статистической избыточности в определенном массиве символов, наоборот, оно ориентировано на внесение в данный массив избыточных символов, которые позволяют трансформировать диссипативную структуру в функционально определенную алгебраическую систему. В роли такой системы выступает система линейных алгебраических уравнений (СЛАУ) [8]. Ее решение X совместно с хеш-функцией h [7] матрицы коэффициентов A обеспечивает на приемной стороне однозначное восстановление передаваемой информации, но использует для кодирования меньшее количество символов, что и обуславливает отнесение рассматриваемого преобразования к методам сжатия без потерь [6].

Алгоритм функционального сжатия двоичной информации представлен на рисунке 2 и состоит из двух частей: алгоритмов компрессии и декомпрессии.

Особенностью обоих алгоритмов является возможность использования технологий параллельного и асинхронного программирования, что существенно сокращает время выполнения задач компрессии и декомпрессии блоков данных. Тем не менее, объем производимых вычислений достаточно большой и время решения задачи сжатия или расжатия может намного превышать время передачи по сети связи несжатой информации. Следовательно, основной областью применения метода функционального сжатия являются системы управления, оборудованные высокопроизводительными вычислительными комплексами, которые способны осуществлять сжатие информационного потока в режиме реального времени [1, 2].

Преимущество указанной технологии заключается не только в повышении пропускной способности, но и в обеспечении высокого уровня функциональной устойчивости, живучести и скрытности интегрированной системы управления специального назначения, что достигается возможностью перехода на помехозащищенные и скрытные режимы работы средств радиосвязи, как правило, характеризующиеся низкой скоростью

информационного обмена.

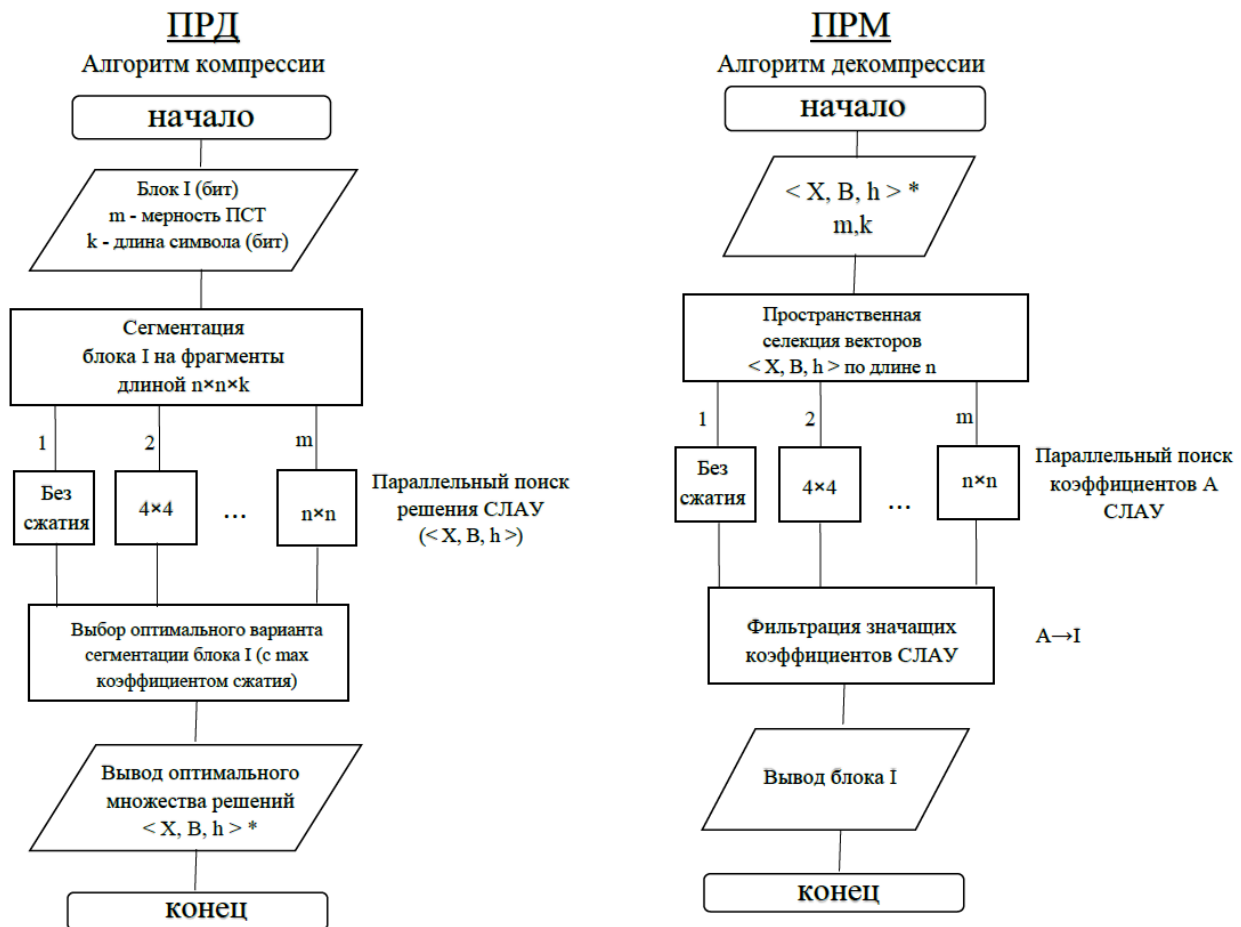


Рисунок 2 – Алгоритм функционального сжатия двоичной информации
(на передающей стороне (ПРД) – алгоритм компрессии, на приемной стороне (ПРМ) – алгоритм декомпрессии)

На рисунке 3 представлена концептуальная схема построения параллельного сетевого тракта (ПСТ) в пакетной сети радиосвязи с многомерной маршрутизацией пакетов (ММП) [3-5].

Как следует из рисунка, основными элементами такой системы передачи информации являются следующие:

- 1) ПЭВМ А(Б) – терминалы автоматизированных рабочих мест должностных лиц в виде персональных электронных вычислительных машин (ПЭВМ), размещенные на пунктах управления А и Б соответственно;
- 2) ТСР – сетевая служба обмена данными на транспортном уровне;
- 3) ММП маршрутизатор А(Б) – многомерные маршрутизаторы, размещенные на пунктах управления А и Б соответственно;
- 4) DPI – сетевая служба глубокого анализа пакетов (необходима для захвата ТСР потока, передаваемого терминалом);
- 5) eТСР – усовершенствованная сетевая служба обмена данными на транспортном уровне (позволяет разбивать захваченный ТСР поток на парциальные потоки в соответствии со структурой ПСТ);
- 6) MPR – сетевая служба оркестрации и управления ММП (необходима для поиска и настройки ПСТ);
- 7) FnC – служба, реализующая функциональное сжатие потока данных;
- 8) tap 1-tap n – виртуальные сетевые интерфейсы, являющиеся точками входа/выхода в ветви ПСТ, которые, в свою очередь, фиксируются статическими маршрутами;
- 9) TR – транзитные маршрутизаторы (коммутаторы), составляющие ветвь ПСТ (статический маршрут).

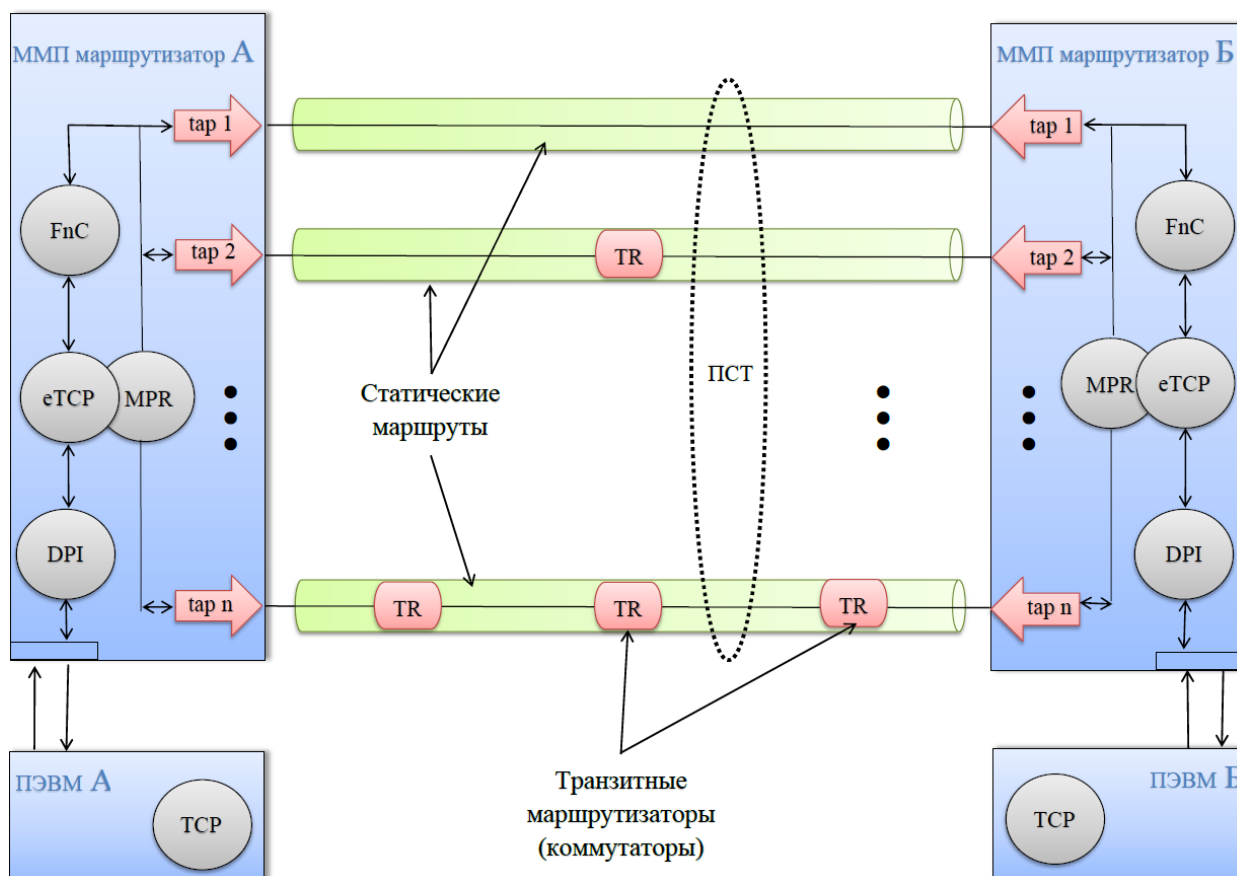


Рисунок 3 – Концептуальная схема построения параллельного сетевого тракта в пакетной сети радиосвязи с многомерной маршрутизацией пакетов

Использование в сети связи с ММП функционального сжатия (FnC) наиболее эффективно за счет выравнивания информационных скоростей в разнородных по пропускной способности ветвях тракта, а также пространственного кодирования CTS. При пространственном кодировании CTS его номер не передается по каналу связи, а закрепляется за статическим маршрутом ПСТ, вследствие чего удастся полностью исключить избыточность служебных символов, необходимых для декомпрессии.

Таким образом, в статье представлен новый метод функционального сжатия двоичной информации (FnC), реализация которого в перспективных интегрированных системах управления и пакетных сетях радиосвязи совместно с методом ММП (MPR/eTCP/DPI) позволит существенно повысить их пропускную способность (от 10 до 30%) при рациональном использовании имеющихся аппаратно-программных ресурсов.

Литература

- Орехов С.Е., Артамонов Д.П., Иванов С.А. Технологии облачных вычислений в интегрированных системах управления // Инфокоммуникационные технологии. – 2020. – Т. 18. – № 4. – С. 477-484.
- Орехов С.Е., Лобанов А.В., Матвеев Е.Ю., Семенов А.Л. Методологические аспекты совершенствования перспективных информационно-коммуникационных узлов, предназначенных для решения высокопроизводительных задач на основе облачных технологий // Электронный научный журнал «Век качества». – 2020. – №1. – С. 142-157.
- Орехов С.Е., Ваганов И.Н. Концептуальная модель пакетной сети радиосвязи метрового диапазона с многомерными маршрутами передачи сообщений // Известия Института инженерной физики. – 2009. – №1 (11). – С. 57-61.
- Орехов С.Е., Сысоев И.В. Оптимизация распределения TCP нагрузки по параллельному сетевому тракту сети связи с многомерной маршрутизацией пакетов // Известия Института инженерной физики. – 2014. – №1 (31). – С. 57-59.

- Орехов С.Е. Численный метод анализа временных характеристик случайного процесса,

описываемого поглощающей конечной марковской цепью с неоднородными по длительности шагами переходов между состояниями цепи // Известия Института инженерной физики. – 2013. – №3 (29). – С. 62-65.

6. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ-МИФИ, 2003. – 384 с.
7. Aumasson J.P. Serious cryptography. A practical introduction to modern encryption. – San Francisco: No starch press, 2018. – 433 p.
8. Lal R. Algebra 2. Linear algebra, Galois Theory, Representation Theory, Group Extensions and Schur Multiplier. – Singapore: Springer Nature, 2017. – 439 p.

IMPROVING THE CAPACITY OF A PROSPECTIVE PACKET RADIO NETWORK BASED ON THE FUNCTIONAL COMPRESSION METHOD AND MULTIDIMENSIONAL PACKET ROUTING

Docent, PhD of Engineering Sciences, Orekhov S. E., student Demensky D. S.

Peter the Great Military Academy of the Strategic Missile Forces
(Branch in the city of Serpukhov Moscow region)

The article discusses the main ways to improve the capacity of a promising packet radio network, including a direction focused on effective compression of data transmitted over communication channels. The principle and content of a new method for functional compression of binary information are presented, which allows for increasing the capacity of a promising packet radio network by compressing statistically aligned data. In addition, options for implementing the functional compression algorithm for binary information are proposed within the framework of a conceptual scheme for building a parallel network path in a communication network with multidimensional packet routing, which significantly improves the capacity of a promising packet radio network while efficiently utilizing available hardware and software resources.



МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЦЕССА ПРИНЯТИЯ РЕШЕНИЯ ОПЕРАТОРОМ АСУ С ПОДДЕРЖКОЙ ПРИНЯТИЯ РЕШЕНИЯ НА БАЗЕ КОНЕЧНОЙ ЦЕПИ МАРКОВА

д.т.н., доц. Попов М.Ю.¹, к.т.н. Девятяров В.Б.²,
к.т.н. Слободсков О.Е.³, к.т.н. Реджепов И.В.¹

¹Филиал военной академии РВСН имени Петра Великого,

²АО «Корпорация «Московский институт теплотехники»,.

³АО «Российский институт мощного радиостроения»,.

В статье представлена математическая модель процесса принятия решения оператором автоматизированной системы управления с поддержкой принятия решения. Модель создана на базе конечной цепи Маркова и описывает трехальтернативный поэтапный процесс принятия решения оператором. В программной среде для решения задач Mathcad представлены этапы модели.

Оператор автоматизированной системы управления (АСУ) с поддержкой принятия решения (ППР) принимает решение, по отработке поступившего на терминальное устройство автоматизированного рабочего места (АРМ) сообщения, поэтапно [1], с учетом дополнительной информации от системы, которая корректирует вероятностно-временной уклон выработки им решения. Такой процесс формализован в виде поглощающей конечной марковской цепи (ПКМЦ), граф состояний и переходов (ГСП) которой представлен на рисунке 1.

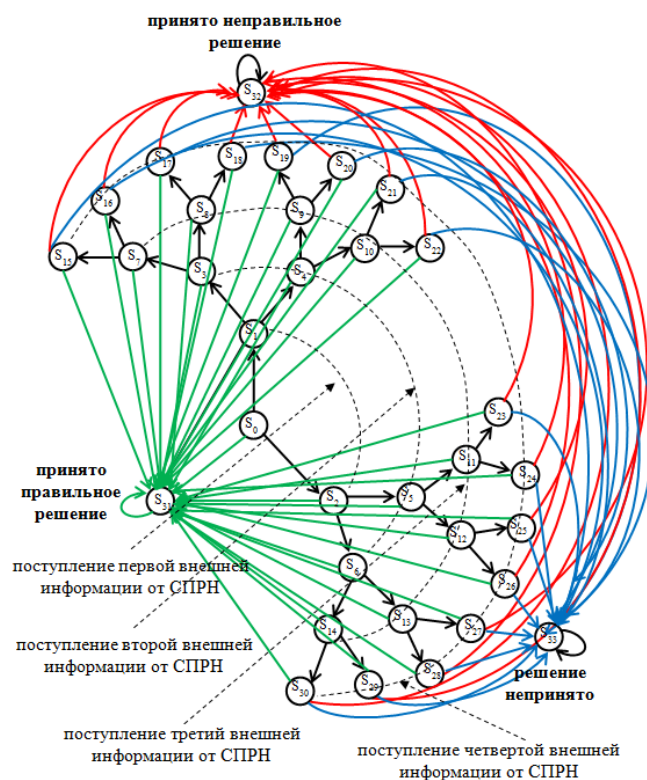


Рисунок 1. ПКМЦ процесса принятия решения

Физический смысл состояний цепи таков: S_0 - состояние, соответствующее поступлению сообщения, оператор начал формирования решения по его отработке; S_1 - на первом этапе принятия решения (ЭПР) оператором не принято решение; S_2 - на первом ЭПР оператором принято неправильное решение; S_3, S_6 - на втором ЭПР оператором не принято решение; S_4, S_5 - на втором ЭПР оператором принято неправильное решение; S_7, S_9, S_{11}, S_{13} - на третьем ЭПР оператором не принято решение; $S_8, S_{10}, S_{12}, S_{14}$ - на третьем ЭПР оператором принято неправильное решение; $S_{15}, S_{17}, S_{19}, S_{21}, S_{23}, S_{25}, S_{27}, S_{29}$ - на четвертом ЭПР оператором не принято решение; $S_{16}, S_{18}, S_{20}, S_{22}, S_{24}, S_{26}, S_{28}, S_{30}$ - на третьем ЭПР оператором принято неправильное решение; S_{31}, S_{32}, S_{33} - состояния, соответствующие принятию оператором правильного, неправильного решения и неприятию оператором решения, соответственно - поглощающие состояния.

Матрицы переходных вероятностей (МПВ) и шагов переходов (МШП) имеют вид:

$$P_{[34,34]} = \begin{bmatrix} 0 & p_{0,1} & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & p_{33,33} \end{bmatrix}, \quad T_{[34,34]} = \begin{bmatrix} 0 & \tau_{0,1} & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \tau_{33,33} \end{bmatrix}. \quad (1)$$

Марковская цепь будет являться неоднородной [2,3] в следствии изменяемых МПВ и МШП на шагах процесса, в силу «коррекции» значений переходных вероятностей (ПВ) и шагов переходов (ШП) в моменты получения дополнительной информации от системы ППР.

В программной среде для решения задач Mathcad была реализована модель процесса принятия решения оператором АСУ с ППР обеспечивающая расчет вероятностно-временных характеристик (ВВХ) и временных характеристик (ВХ) процесса [4,5], этапы ее таковы.

Этап 1. Задание исходных данных моделирования.

z_c - количество шагов процесса моделирования, [шт.]; $P_{pr(5)}$ и $P_{npr(5)}$ - вектор-строки из 5 элементов с вероятностями принятия оператором правильного решения и непринятия оператором решения на ЭПР, соответственно; $T_{r(5)}$ - вектор-строка из 5 элементов - времен ЭПР, [сек.]; $\tau_{\min}$ - минимальное время события процесса (минимальный ШП цепи), [сек.]; $P_{S(34)}^{(0)} = \|P_{S_0}^{(0)}; P_{S_1}^{(0)}; P_{S_2}^{(0)}; \dots; P_{S_{33}}^{(0)}\|$ - вектор-строка вероятностей состояний цепи на 0 шаге процесса – вектор начальных состояний (ВНС) - схема начала организации процесса:

$$P_{S(34)}^{(0)} = \|1; 0; 0; \dots; 0\| = P_{(34)}^{(0)}. \quad (2)$$

Сочетания соответствующих элементов $P_{pr(5)}$, $P_{npr(5)}$ и $T_{r(5)}$ формирует вероятностно-временной уклон процесса принятия решения оператором.

Этап 2. Определение ШП и ПВ ПКМЦ.

2.1 Определение ШП цепи.

$$\begin{aligned} [T_r]_{0,0} &= \tau_{0,31} = \tau_{0,1} = \tau_{0,2}; \\ [T_r]_{0,1} &= \tau_{1,31} = \tau_{1,3} = \tau_{1,4} = \tau_{2,31} = \tau_{2,5} = \tau_{2,6}; \\ [T_r]_{0,2} &= \tau_{3,31} = \tau_{3,7} = \tau_{3,8} = \tau_{4,31} = \tau_{4,9} = \tau_{4,10} = \tau_{5,31} = \tau_{5,11} = \tau_{5,12} = \tau_{6,31} = \tau_{6,13} = \tau_{6,14}; \\ [T_r]_{0,3} &= \tau_{7,31} = \tau_{7,15} = \tau_{7,16} = \tau_{8,31} = \tau_{8,17} = \tau_{8,18} = \tau_{9,31} = \tau_{9,19} = \tau_{9,20} = \tau_{10,31} = \tau_{10,21} = \tau_{10,22} = \\ &= \tau_{11,31} = \tau_{11,23} = \tau_{11,24} = \tau_{12,31} = \tau_{12,25} = \tau_{12,26} = \tau_{13,31} = \tau_{13,27} = \tau_{13,28} = \tau_{14,31} = \tau_{14,29} = \tau_{14,30}; \\ [T_r]_{0,4} &= \tau_{15,31} = \tau_{15,32} = \tau_{15,33} = \tau_{16,31} = \tau_{16,32} = \tau_{16,33} = \tau_{17,31} = \tau_{17,32} = \tau_{17,33} = \tau_{18,31} = \tau_{18,32} = \\ &= \tau_{18,33} = \tau_{19,31} = \tau_{19,32} = \tau_{19,33} = \tau_{20,31} = \tau_{20,32} = \tau_{20,33} = \tau_{21,31} = \tau_{21,32} = \tau_{21,33} = \tau_{22,31} = \tau_{22,32} = \\ &= \tau_{22,33} = \tau_{23,31} = \tau_{23,32} = \tau_{23,33} = \tau_{24,31} = \tau_{24,32} = \tau_{24,33} = \tau_{25,31} = \tau_{25,32} = \tau_{25,33} = \tau_{26,31} = \tau_{26,32} = \\ &= \tau_{26,33} = \tau_{27,31} = \tau_{27,32} = \tau_{27,33} = \tau_{28,31} = \tau_{28,32} = \tau_{28,33} = \tau_{29,31} = \tau_{29,32} = \tau_{29,33} = \tau_{30,31} = \tau_{30,32} = \tau_{30,33}; \\ \tau_{\min} &= \tau_{31,31} = \tau_{32,32} = \tau_{33,33}. \end{aligned}$$

где $[\cdot]_{0,0}$ - процедура выделения элемента матрицы;

2.2 Определение ПВ цепи.

ПВ принятия правильного решения оператором до получения внешней информации и после получения первой, второй, третьей, четвертой внешней информации, соответственно, таковы:

$$\begin{aligned} [P_{pr}]_{0,0} &= p_{0,31}; \\ [P_{pr}]_{0,1} &= p_{1,31} = p_{2,31}; \\ [P_{pr}]_{0,2} &= p_{3,31} = p_{4,31} = p_{5,31} = p_{6,31}; \\ [P_{pr}]_{0,3} &= p_{7,31} = p_{8,31} = p_{9,31} = p_{10,31} = p_{11,31} = p_{12,31} = p_{13,31} = p_{14,31}; \\ [P_{pr}]_{0,4} &= p_{15,31} = p_{16,31} = p_{17,31} = p_{18,31} = p_{19,31} = p_{20,31} = p_{21,31} = p_{22,31} = p_{23,31} = p_{24,31} = p_{25,31} = \\ &= p_{26,31} = p_{27,31} = p_{28,31} = p_{29,31} = p_{30,31}. \end{aligned}$$

ПВ неприятия решения оператором до получения внешней информации и после получения первой, второй, третьей, четвертой внешней информации, соответственно, таковы:

$$\begin{aligned} [P_{npr}]_{0,0} &= p_{0,1}; \\ [P_{npr}]_{0,1} &= p_{1,3} = p_{2,6}; \\ [P_{npr}]_{0,2} &= p_{3,7} = p_{4,9} = p_{5,11} = p_{6,13}; \\ [P_{npr}]_{0,3} &= p_{7,15} = p_{8,17} = p_{9,19} = p_{10,21} = p_{11,23} = p_{12,25} = p_{13,27} = p_{14,29}; \\ [P_{npr}]_{0,4} &= p_{15,33} = p_{16,33} = p_{17,33} = p_{18,33} = p_{19,33} = p_{20,33} = p_{21,33} = p_{22,33} = p_{23,33} = p_{24,33} = p_{25,33} = \\ &= p_{26,33} = p_{27,33} = p_{28,33} = p_{29,33} = p_{30,33}. \end{aligned}$$

ПВ принятия неправильного решения оператором до получения внешней информации и после получения первой, второй, третьей, четвертой внешней информации, соответственно, таковы:

$$\begin{aligned} 1 - p_{0,31} - p_{0,1} &= p_{0,2}; \\ 1 - p_{1,31} - p_{1,3} &= p_{1,4} = p_{2,5}; \\ 1 - p_{3,31} - p_{3,7} &= p_{3,8} = p_{4,10} = p_{5,12} = p_{6,14}; \\ 1 - p_{7,31} - p_{7,15} &= p_{7,16} = p_{8,18} = p_{9,20} = p_{10,22} = p_{11,24} = p_{12,26} = p_{13,28} = p_{14,30}; \\ 1 - p_{15,31} - p_{15,33} &= p_{15,32} = p_{16,32} = p_{17,32} = p_{18,32} = p_{19,32} = p_{20,32} = p_{21,32} = p_{22,32} = p_{23,32} = \\ &= p_{24,32} = p_{25,32} = p_{26,32} = p_{27,32} = p_{28,32} = p_{29,32} = p_{30,32}. \end{aligned}$$

Этап 3. Формирование МПВ $P_{[34,34]}$ из ПВ цепи.

3.1 Проверка стохастичности МПВ.

Проверка условия:

$$\sum (P_{[34,34]}^T)^{(s)^T} = \begin{Bmatrix} 1 \\ 1 \\ \dots \\ 1 \end{Bmatrix}, \quad (3)$$

где $[.]^T$ - процедура транспонирования;

$[.]^{(s)^T}$ - процедура выделение строки из матрицы;

$\sum$ - процедура суммирования элементов строк матрицы;

$s = (\overline{0,33})$ - номера строк матрицы.

Выражение (3) формирует вектор-столбец, элементы которого должны принимать значение 1. Если это не так, то необходимо подвергнуть анализу порядок и логику формирования ПВ в части обеспечения полной группы событий - осуществить возврат к этапу 2.2.

Этап 4. Формирование МШП $T_{[34,34]}$ из ШП цепи.

Этап 5. Формирование вектора-столбца частных средних шагов перехода.

Элементы вектора находится как сумма произведений соответствующих ПВ и ШП, то есть:

$$t_{S(34)} = \begin{Bmatrix} t_{S_0} \\ t_{S_1} \\ t_{S_2} \\ t_{S_3} \\ \dots \\ t_{S_{33}} \end{Bmatrix} = \begin{Bmatrix} p_{0,1} \cdot \tau_{0,1} + p_{0,2} \cdot \tau_{0,2} + p_{0,31} \cdot \tau_{0,31} \\ p_{1,3} \cdot \tau_{1,3} + p_{1,4} \cdot \tau_{1,4} + p_{1,31} \cdot \tau_{1,31} \\ p_{2,5} \cdot \tau_{2,5} + p_{2,6} \cdot \tau_{2,6} + p_{2,31} \cdot \tau_{2,31} \\ p_{3,7} \cdot \tau_{3,7} + p_{3,8} \cdot \tau_{3,8} + p_{3,31} \cdot \tau_{3,31} \\ \dots \\ p_{33,33} \cdot \tau_{33,33} \end{Bmatrix}. \quad (4)$$

Этап 6. Формирование единой оси времени процесса.

6.1 Формирование средних шагов перехода:

$$T(sh) = \left[\left[\left[P_{(34)}^{(0)} \cdot (P_{[34,34]})^{sh} \right]^T \right]^{(0)^T} \right] \cdot t_{S_{(34)}}, \quad (5)$$

$\left[\left[\left[P_{(34)}^{(0)} \cdot (P_{[34,34]})^{sh} \right]^T \right]^{(0)^T} \right]$ - вектор-строка – результат решения уравнения Колмогорова-

Чепмена;

$sh = (0, zc)$ - шаги процесса.

Элементы $T(sh)$ - средние ШП, соответствующие шагам процесса.

6.2 Создание функции шагов процесса:

$$f_0(i, j) = (j). \quad (6)$$

6.3 Создание матрицы размером $[1, zc + 1]$:

$$sh = matrix(1, zc + 1, f_0), \quad (7)$$

где $matrix[\cdot]$ - процедура формирования матрицы;

1 – количество строк;

$zc + 1$ - количество столбцов;

f_0 - функция, определяющая правило формирования элементов матрицы.

Теперь sh представляет собой вектор-строку, каждый элемент которого есть шаг процесса моделирования.

6.4 Создание функции, формирующей времена протекания процесса, соответствующие шагу процесса моделирования:

$$f(i, j) = \left(\sum_{i=0}^j T(i) \right). \quad (8)$$

6.5 Формирование единой оси времени:

$$eov = matrix(1, zc + 1, f) \quad (9)$$

- вектор-строка, элементы которого есть времена, затрачиваемые процессом, соответствующие шагу процесса моделирования цепи.

Этап 7. Нахождение BBX процесса в динамике шагов процесса.

Нахождение BBX процесса определяются динамикой вероятности состояния S_{31} цепи во времени.

7.1 Создание функции, формирующей динамику вероятности S_{31} , осуществляется так:

$$f1(i, j) = \left[P_{(34)}^{(0)} \cdot (P_{[34,34]})^j \right]_{0,31}. \quad (10)$$

7.2 Создания матрицы-строки, элементы которой есть вероятности нахождения цепи в S_{31} в зависимости от ШП:

$$VVHi_o = matrix(1, zc + 1, f1). \quad (11)$$

Этап 8. Проверка достаточности заданного исследователем количества шагов процесса моделирования zc .

Этап 9. Определение BBX процесса в динамике времени.

BBX в динамике времени можно интерпретировать как соответствие элементов вектора-строки $VVHpr$ с соответствующими элементами eov . Причем: $\max(VVHpr)$, $\max(VVHnpr)$, $\max(VVHrn)$ - максимальные значения вероятностей нахождения цепи в состояниях S_{31} , S_{32} , S_{33} , соответственно; $\max(eov)$ - максимальное значение времени моделирования процесса соответствующее $\max(VVHpr)$, $\max(VVHnpr)$, $\max(VVHrn)$, где $\max(\cdot)$ - процедура нахождения максимального значения элементов матрицы.

Этап 10. Определение BX процесса.

Средне время принятия решения и СКО времени есть $[1-4]$:

$$\hat{M}(t) = \sum_{sh=0}^{zc} sh \cdot T(sh) \cdot \left(\left[\left[\left(P_{[34,34]} \right)^{sh+1} \right]^T \right]^{(0)^T} \right]_{0,33} - \left[\left[\left(P_{[34,34]} \right)^{sh} \right]^T \right]^{(0)^T} \right]_{0,33} \right); \quad (12)$$

$$\hat{\sigma}(t) = \sqrt{\sum_{sh=0}^{zc} \left(\left[\left[\left(P_{[34,34]} \right)^{sh+1} \right]^T \right]^{(0)^T} \right]_{0,33} - \left[\left[\left(P_{[34,34]} \right)^{sh} \right]^T \right]^{(0)^T} \right]_{0,33} \cdot [T(sh) \cdot sh - \hat{M}(t)]^2}. \quad (13)$$

На рисунке 2 представлен график расчета BBX и VX процесса принятия оператором решения для следующих исходных данных: $zc = 5$, [шт.]; $P_{pr(5)} = (0,1;0,2;0,3;0,4;0,5)$; $P_{npr(5)} = (0,5;0,4;0,3;0,2;0,1)$; $T_{r(5)} = (5;15;30;45;60)$, [сек.]; $\tau_{min} = 0,001$, [сек.].

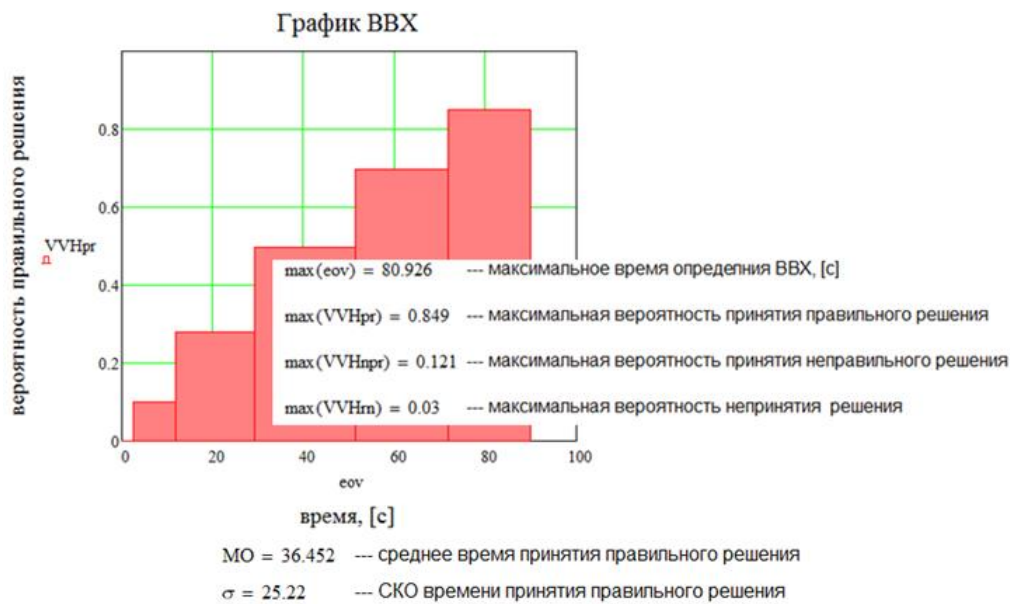


Рисунок 2. Расчет BBX и VX процесса принятия оператором решения

Таким образом, на базе ПКМЦ создана и реализована в программной среде для решения задач Mathcad математическая модель процесса принятия решения оператором АРМ АСУ с ППР. Модель служит инструментом исследования BBX и VX процесса [1-4] принятия решения оператором, предусматривает анализ ее чувствительности к входным параметрам.

Литература

1. Программа расчета численных характеристик поглощающей конечной полумарковской цепи торбенко я. к., попов м. ю., девятыров в. б., киреев д. а., харитонов и. а. свидетельство о регистрации программы для эвм 2025612813, 04.02.2025. заявка от 14.11.2024.
2. Аналитические выражения и программные средства определения числовых характеристик конечных цепей маркова попов м. ю., девятыров в. б., слободсков о. е., харитонов и. а. проектирование и технология электронных средств. 2025. № 1 . с. 48 - 57.
3. Определение показателей динамики процесса, формализованного поглощающей или регулярной конечной полумарковской цепью в зависимости от времени на базе языка программирования с++ в среде visual studio попов м. ю., калганов е. в., асанов а. с., харитонов и. а. в сборнике: радиоэлектронные устройства и системы для инфокоммуникационных технологий ("рэус-ит 2024"). доклады всероссийской конференции, посвященной дню радио. москва, 2024. с. 114 - 118.
4. Программа расчета численных характеристик поглощающей конечной полумарковской цепи на базе языка программирования с++ в среде visual studio попов м. ю., девятыров в. б., иванов и. б., киреев д.а., харитонов и.а. в сборнике: современные технологии обработки сигналов (стос-2023). доклады 4-ой всероссийской конференции. москва, 2023. с. 42 - 47.

5. Конечная полумарковская цепь, описывающая процесс обработки оператором автоматизированного рабочего места асу поступившего по радиоканалу сообщения попов м. ю., илющенко в. в., пономарев а. м., калач п. к., киреев д. а. в сборнике: цифровая обработка сигналов и её применение (dspra-2022). 24-я международная конференция. москва, 2022. с. 21 - 25.

MATHEMATICAL MODEL OF PROCESS OF DECISION-MAKING BY THE OPERATOR OF THE AUTOMATED CONTROL SYSTEM WITH SUPPORT OF DECISION-MAKING ON THE BASIS OF FINAL MARKOV CHAIN

Dr.Sci.Tech. Popov M.Yu.¹, Cand.Tech.Sci. Devyatiyarov V.B.²,
Cand.Tech.Sci. Slobodskov O.E.³, Cand.Tech.Sci. Redzhepov I.V.¹

¹Branch of military academy of Rocket strategic forces of a name of Peter the Great
(с. Serpukhov, Moscow region).

²Joint-stock company corporation «Moscow institute of heat engineering».

³The Russian institute of a powerful radio structure, St.-Petersburg.

In article the mathematical model of process of decision-making by the operator of the automated control system with decision-making support is presented. The model is created on the basis of final Markov chain and describes three-alternative stage-by-stage process of decision-making by the operator. In the program environment for the decision of problems Mathcad model stages are presented.



УПРАВЛЕНИЕ ПАРАМЕТРАМИ КАНАЛА СПУТНИКОВОЙ СВЯЗИ С ГЕОСТАЦИОНАРНЫМ КОСМИЧЕСКИМ АППАРАТОМ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

студ. Саакян Э.А.

Московский технический университет связи и информатики

В статье рассматривается задача интеллектуального управления параметрами канала спутниковой связи с геостационарным космическим аппаратом на основе методов машинного обучения. Актуальность исследования обусловлена необходимостью повышения пропускной способности, энергетической эффективности и устойчивости спутниковых систем при работе в условиях переменного состояния канала.

Для геостационарных линий связи характерны значительные потери в свободном пространстве, большая задержка распространения сигнала и заметное влияние атмосферных факторов, прежде всего дождевого затухания в Ku- и Ka-диапазонах. Показано, что традиционные пороговые методы адаптации, основанные на фиксированных правилах выбора режимов модуляции и кодирования, не всегда обеспечивают оптимальный баланс между надежностью и скоростью передачи. Обоснована возможность применения алгоритмов машинного обучения для выбора параметров передачи по совокупности эксплуатационных и метеорологических признаков.

Введение

Системы спутниковой связи с использованием геостационарных космических аппаратов занимают важное место в современной инфокоммуникационной инфраструктуре. Они применяются для телевидения, ведомственной и корпоративной связи, организации широкополосного доступа, построения резервных магистральных каналов и обеспечения связи в удаленных регионах. Преимущество GEO-аппаратов заключается в постоянстве положения относительно наземного наблюдателя, что упрощает наведение антенн и позволяет формировать устойчивые зоны покрытия [1-2].

Вместе с тем канал связи с геостационарным спутником обладает рядом особенностей, усложняющих управление параметрами передачи. К ним относятся большая длина трассы, значительные потери в свободном пространстве, задержка распространения сигнала и чувствительность высокочастотных диапазонов к атмосферным возмущениям. Особенно заметно это проявляется при работе в Ku- и Ka-диапазонах, где осадки, облачность и поглощение в атмосфере могут приводить к существенному ухудшению отношения сигнал/шум и увеличению вероятности ошибок [3].

Традиционные методы управления параметрами канала обычно используют фиксированные пороги SNR и BER, по достижении которых система переключается между допустимыми режимами модуляции, кодирования и мощности. Такой подход технологически прост и широко применяется в существующих стандартах, однако он не учитывает сложную нелинейную зависимость качества канала от множества факторов, включая загрузку системы, особенности трафика и метеорологическую обстановку. В связи с этим возрастает интерес к использованию методов машинного обучения, способных принимать решения на основе более полного набора признаков и статистики реальной эксплуатации [4].

Целью статьи является анализ возможностей управления параметрами канала спутниковой связи с геостационарным космическим аппаратом на основе методов машинного обучения, а также формирование обобщенной модели интеллектуального выбора режимов передачи в условиях изменяющегося состояния линии связи.

Особенности GEO-канала как объекта управления

Канал спутниковой связи с геостационарным космическим аппаратом представляет собой сложный технический объект, параметры которого изменяются под действием как аппаратурных, так и внешних факторов. Наиболее существенными характеристиками являются отношение сигнал/шум, уровень принимаемой мощности, вероятность битовой ошибки, доступность канала, спектральная эффективность и энергетический запас линии. Между этими величинами существует взаимосвязь: повышение устойчивости канала обычно достигается ценой снижения скорости полезной передачи или увеличения энергетических затрат [5].

При эксплуатации GEO-систем важную роль играет дождевое затухание. Его влияние особенно велико в высокочастотных диапазонах, где даже кратковременные интенсивные осадки способны вызвать заметное ослабление сигнала. В таких условиях использование статических режимов передачи

оказывается неэффективным, поскольку система либо расходует избыточный энергетический ресурс, либо не успевает своевременно перейти на более устойчивую конфигурацию [6].

Для эффективного управления необходимо учитывать не только текущее измеренное состояние канала, но и сопутствующие признаки: интенсивность осадков, тип трафика, загрузку транспондера, рабочий диапазон частот, требования к качеству обслуживания, а также накопленную статистику изменения параметров линии. Это переводит задачу из области простого порогового регулирования в область многопараметрического принятия решений [7].

Традиционные методы адаптации параметров передачи

В современных спутниковых системах наиболее известными средствами адаптации служат АСМ и VCM, реализуемые в стандартах DVB-S2 и DVB-S2X. Их применение позволяет изменять комбинации модуляции и кодовой скорости в зависимости от качества принимаемого сигнала. На инженерном уровне это означает выбор режима MODCOD, соответствующего определенному диапазону SNR [8].

Преимущество такого подхода состоит в простоте, надежности и понятности алгоритма. Пороговые значения задаются заранее, а поведение системы оказывается предсказуемым. Однако у него имеются и очевидные недостатки. Во-первых, решение часто принимается по ограниченному набору параметров. Во-вторых, пороги обычно выбираются с запасом, чтобы исключить критические ошибки, а это снижает спектральную эффективность. В-третьих, система в основном реагирует на уже возникшее ухудшение канала, а не прогнозирует его [9].

Для GEO-каналов, где задержка велика, а влияние метеофакторов способно быстро изменять энергетический баланс линии, такой подход недостаточно гибок. Следовательно, необходим алгоритм, способный учитывать большее число наблюдаемых параметров и строить решение с учетом вероятного развития ситуации в ближайшем интервале времени [10].

Применение машинного обучения в управлении параметрами GEO-канала

Методы машинного обучения позволяют формализовать задачу выбора параметров передачи как задачу классификации, регрессии или последовательного принятия решений. В простейшем варианте модель классификации сопоставляет текущему состоянию канала один из допустимых режимов передачи. Регрессионный подход ориентирован на прогноз значений SNR, BER или глубины затухания. Более сложная схема основана на обучении с подкреплением, когда агент последовательно выбирает действия, максимизируя функцию полезности, зависящую от пропускной способности, надежности и энергопотребления [11].

В качестве входных признаков модели могут использоваться SNR, BER, уровень принимаемой мощности, интенсивность осадков, данные о погоде, диапазон частот, загрузка канала, тип сервиса и требования QoS. На выходе алгоритм формирует рекомендации по выбору модуляции, кодовой скорости, мощности передатчика и при необходимости символьной скорости. Преимущество такого подхода заключается в возможности выявлять нелинейные зависимости, которые отсутствуют в пороговых таблицах [12].

Для практического применения особенно важны модели, сочетающие достаточную точность с интерпретируемостью. В инженерных системах связи полезны решающие деревья, случайный лес, градиентный бустинг и гибридные схемы, где статистическая модель дополняет физические представления о канале. В задачах, где требуется упреждающая адаптация, перспективны методы обучения с подкреплением и прогнозирования временных рядов [13].

Таблица 1

Сравнение традиционного и интеллектуального подхода к управлению параметрами [8]

Критерий	Традиционный пороговый подход	Подход на основе машинного обучения
Основа принятия решения	Фиксированные правила и таблицы	Обученная модель
Число учитываемых факторов	Небольшое	Многомерное
Тип адаптации	Реактивный	Реактивно-прогнозный
Спектральная	Средняя	Потенциально выше

эффективность		
Требования к данным	Низкие	Повышенные
Вычислительная сложность	Низкая	Средняя или высокая
Интерпретируемость	Высокая	Зависит от модели

Таблица 1 показывает, что методы машинного обучения не отменяют инженерных принципов адаптации, а расширяют их возможности за счет анализа большего объема данных. Наиболее рациональным представляется гибридный вариант, при котором предельные режимы задаются стандартом, а конкретный выбор внутри допустимой области выполняется интеллектуальным алгоритмом [11].

Концептуальная схема управления параметрами передачи

Рассмотрена задача адаптации в виде отображения «состояние канала – управляющее решение». Вектор состояния может включать текущие и усредненные значения SNR, BER, уровень принятого сигнала, метеоданные, тип диапазона, загрузку канала и требуемый класс обслуживания.

Целевая функция такого алгоритма должна учитывать несколько критериев одновременно. С одной стороны, требуется максимизировать спектральную эффективность и полезную скорость передачи. С другой стороны, необходимо ограничивать BER, обеспечивать требуемую доступность канала и не выходить за допустимый энергетический бюджет системы. Таким образом, задача имеет многокритериальный характер [14].

С практической точки зрения интеллектуальный алгоритм может работать в двух режимах. В первом режиме он выполняет классификацию состояния канала и выбирает один из заранее разрешенных режимов работы. Во втором режиме модель сначала прогнозирует изменение качества линии, после чего блок оптимизации назначает параметры передачи с учетом ожидаемой динамики. Второй вариант особенно интересен для компенсации метеорологических возмущений в диапазонах, чувствительных к дождевому затуханию [15].

Таблица 2

Состояния канала [5]

Состояние канала	SNR, дБ	Осадки	Рекомендуемый режим	Управляющее воздействие
Благоприятное	> 12	Отсутствуют или слабые	16APSK / 32APSK, высокая кодовая скорость	Максимизация пропускной способности
Умеренно устойчивое	9–12	Слабые–умеренные	8PSK / 16APSK, средняя кодовая скорость	Баланс скорости и надежности
Пограничное	6–9	Умеренные	QPSK / 8PSK, пониженная кодовая скорость	Переход к устойчивому режиму
Неблагоприятное	<6	Сильные	QPSK, низкая кодовая скорость	Минимизация ошибок, возможное увеличение мощности

Приведенная в таблице 2 схема показывает общую логику адаптации: при ухудшении состояния канала система должна переходить к более устойчивым режимам передачи. Отличие интеллектуального подхода состоит в том, что решение принимается не только по текущему SNR, но и по совокупности сопутствующих признаков, характеризующих вероятность дальнейшего ухудшения канала [12].

Представляется гибридный вариант, при котором предельные режимы задаются стандартом, а конкретный выбор внутри допустимой области выполняется интеллектуальным алгоритмом [11].

Вывод

Управление параметрами канала спутниковой связи с геостационарным космическим аппаратом с применением методов машинного обучения следует рассматривать как одно из наиболее перспективных направлений совершенствования современных спутниковых систем связи. Интерес к данному подходу обусловлен тем, что он позволяет принимать решения на основе совокупности взаимосвязанных параметров, характеризующих текущее состояние канала, а не опираться только на отдельные мгновенные измерения. Практическая ценность такого подхода особенно заметна в тех системах, где качество связи существенно зависит от метеорологических условий, уровня загрузки ресурсов и изменчивости энергетических характеристик линии. В подобных случаях более точная адаптация режимов передачи дает возможность повысить спектральную эффективность, сохранить требуемую доступность канала и рациональнее использовать энергетический ресурс системы. Вместе с тем внедрение таких решений требует аккуратного формирования обучающих выборок, достоверной проверки моделей на реальных или близких к реальным сценариях, а также построения гибридных схем управления, в которых алгоритмы машинного обучения применяются совместно с проверенными инженерными механизмами адаптации.

Для максимальной реализации потенциала ИИ в управлении каналами связи КА рекомендуется дальнейшая работа по созданию гибридных систем, сочетающих элементы ИИ с традиционными протоколами, а также разработка специализированных аппаратных ускорителей для ИИ-алгоритмов, что позволит обеспечить работу в режиме реального времени при минимальных вычислительных затратах.

Литература

1. Саакян, Э. А. Применение искусственного алгоритма управления параметрами канала связи с геостационарным космическим аппаратом // Технологии информационного общества. 2026
2. Либеровский Н.Ю., Припутин В.С., Чиров Д.С. Обзор исследований адаптивного формирования диаграммы направленности и цифровой обработки сигналов // Научные технологии в космических исследованиях Земли. 2021. Т. 13. № 6. С. 1621. doi: 10.36724/2409541920211361621;
3. Марал, Ж. Системы спутниковой связи: системы, методы и технологии / Ж. Марал, М. Буске, Ч. Сун. 6-е изд. Chichester: Wiley, 2020
4. Саттон, Р. С. Обучение с подкреплением: введение / Р. С. Саттон, Э. Г. Барто. 2-е изд. Cambridge, MA: MIT Press, 2018
5. Прокис, Дж. Цифровая связь / Дж. Прокис, М. Салехи. 5-е изд. New York: McGraw-Hill, 2008
6. Рекомендация ITU-R P.618. Данные о распространении и методы прогнозирования, необходимые для проектирования земно-космических телекоммуникационных систем
7. Голдсмит, А. Беспроводные коммуникации. Cambridge: Cambridge University Press, 2005
8. ETSI EN 302 307-2. Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broadband satellite applications. Part II: DVB-S2 Extensions (DVB-S2X)
9. Родди, Д. Спутниковая связь. 4-е изд. New York: McGraw-Hill, 2006
10. Бишоп, К. М. Распознавание образов и машинное обучение. New York: Springer, 2006
11. Мерфи, К. П. Машинное обучение: вероятностный подход. Cambridge, MA: MIT Press, 2012
12. Хейкин, С. Системы связи. 5-е изд. New York: Wiley, 2009
13. Рекомендация ITU-R P.838. Модель удельного ослабления в дожде для использования в методах прогнозирования

14. Скляр, Б. Цифровая связь: основы и приложения. 2-е изд. Upper Saddle River: Prentice Hall, 2001
15. Рекомендация ITU-R P.840. Ослабление вследствие облаков и тумана

CONTROL OF SATELLITE COMMUNICATION CHANNEL PARAMETERS WITH A GEOSTATIONARY SPACECRAFT BASED ON MACHINE LEARNING METHODS

student Saakyan E.A.

Technical University of Communications and Informatics

The article considers the problem of intelligent control of the parameters of a satellite communication channel with a geostationary spacecraft based on machine learning methods. The relevance of the study is due to the need to increase the bandwidth, energy efficiency and stability of satellite systems when operating in a variable channel condition.

Geostationary communication lines are characterized by significant losses in free space, a large delay in signal propagation, and a noticeable effect of atmospheric factors, primarily rain attenuation in the Ku and Ka bands. It is shown that traditional threshold adaptation methods based on fixed rules for selecting modulation and encoding modes do not always provide an optimal balance between reliability and transmission speed. The possibility of using machine learning algorithms to select transmission parameters based on a set of operational and meteorological features is substantiated.



ТЕОРЕТИЧЕСКИЕ ОСНОВЫ И КОНЦЕПЦИЯ ДЕДУКТИВНОЙ ОБРАБОТКИ ЦИФРОВЫХ СИГНАЛОВ

инж. Буров Ю.Я.¹, ст. преп. Бурова А.Ю.²

¹ РНТОРЭС имени А. С. Попова,

² Московский авиационный институт (национальный исследовательский университет)

Рассмотрены вопросы, связанные с исследованием возможностей цифровизации алгоритмов обработки результатов измерений и контроля без применения алгоритмических операций умножения. Актуальность этого исследования обусловлена различной аппаратнозатратностью цифровых реализаций разных арифметических операций, выполнение которых необходимо для преобразования сигналов. Цель исследования – разработка концепции их дедуктивной цифровой обработки. При исследовании использовались методы математического и программного моделирования цифровых сигналов и алгоритмов. Результаты исследования показали и подтвердили преимущества дедуктивной обработки таких сигналов. Разработана и описана её концепция. Определены теоретические основы этой цифровой обработки и области применения её алгоритмов для обработки результатов измерений и контроля.

Введение

Дедуктивная (от лат. «*deductio*» – «вычет», «вычитание») обработка цифровых сигналов – это информационные технологии, связанные с обработкой таких сигналов на основе численных методов и вычислительных алгоритмов цифровой обработки сигналов с использованием электронной вычислительной техники [1-3].

Такие информационные технологии – это совокупность методов, алгоритмов и программно-аппаратных средств, направленных на анализ цифровых сигналов на основе дедуктивных подходов к их преобразованию и обработке. Под цифровым сигналом понимается любая пронумерованная последовательность чисел (цифровых кодов), в том числе значений оцифрованного аналогового сигнала.

Обработка цифрового сигнала включает разработку алгоритмов, которые используются для улучшения сигнала или извлечения из него полезной информации. Поэтому, под сигналом в цифровой обработке понимают его математическое описание, то есть вещественную функцию, содержащую информацию о структуре и параметрах сигнала. А дедуктивная обработка цифрового сигнала представляет собой информационные технологии для манипуляции цифровыми данными, представляющими этот сигнал, с целью их анализа и преобразования, чтобы обеспечивать снижение аппаратной сложности аппаратно-программной реализации вычислительных алгоритмов цифровой обработки такого сигнала.

Быстро растущие объёмы текущей информации, обрабатываемой бортовыми вычислительными комплексами беспилотных аппаратов актуализируют исследования возможностей снижения аппаратной сложности аппаратно-программного обеспечения цифровых средств обработки сигналов приемо-передатчиков, аудио-приборов и видео-приборов методами дедуктивной обработки цифровых сигналов.

В научной и технической литературе ещё не зафиксировано устоявшегося понятия «дедуктивная обработка цифровых сигналов» как отдельного направления цифровой обработки сигналов и в базовых учебниках по таким темам, как «дискретное преобразование Фурье» и «цифровая фильтрация» термин «дедуктивная обработка цифровых сигналов» пока не встречается. Однако, понятие и термин «дедуктивная обработка цифровых сигналов» были предложены и апробированы на научной сессии Российского научно-технического общества радиотехники, электроники и связи (РНТОРЭС) имени А.С. Попова и на Международной научной конференции по цифровой обработке сигналов, а также использован в научной статье, опубликованной в тематическом сборнике, индексируемом в базе данных рецензируемой научной литературы «*Scopus*» [4-7].

Использованные при этом приращения значений коэффициентов цифровой фильтрации относительно значений предыдущих соседних коэффициентов цифровой получили условные наименования: «приращения коэффициентов» и «разностные коэффициенты» [8-9].

Цель, методы и материалы исследования

Цель исследования – разработка концепции дедуктивной цифровой обработки сигналов.

При исследовании использовались методы математического и программного моделирования цифровых сигналов и алгоритмов.

В качестве материалов исследования были использованы временные последовательности цифровых отсчетов полигармонического сигнала с помеховой составляющей типа «белый шум», рекурсивные и нерекурсивные разностные цифровые фильтры с тривиальными и бинарными разностными коэффициентами различных порядков разности, многоступенчатые цифровые анализаторы спектра с

переменным разрешением по частоте и тривиальными коэффициентами частотного сдвига комплексных сигналов на различных ступенях преобразования Фурье.

Теоретические основы дедуктивной обработки цифровых сигналов

Теоретическими основами дедуктивной обработки цифровых сигналов стали следующие методы:

- метод дискретизации сигналов по теореме Котельникова-Найквиста-Шеннона, согласно которой любой непрерывный сигнал с ограниченным спектром может быть восстановлен однозначно и без потерь по своим дискретным отсчетам, взятым с частотой строго больше удвоенной верхней частоты спектра непрерывного сигнала;
- метод конечных разностей, основанный на замене исходных уравнений разностными схемами, в которых функция непрерывного аргумента приближённо заменяется функцией дискретного аргумента;
- методы Дискретного преобразования Фурье и Рекуррентного Дискретного преобразования Фурье, которое позволяет переходить от временного описания исходного цифрового сигнала к его частотному описанию;
- методы рекурсивной и нерекурсивной фильтрации цифровых сигналов.

Результаты исследования

Результаты исследования показали и подтвердили преимущества дедуктивной обработки таких сигналов. Эта их обработка на основе рекуррентных алгоритмов численных методов сведения прямых вычислений сложных функций к выполнению простых операций сложения и сдвига CORDIC (COordinate Rotation DIgital Computer) и разностной цифровой фильтрации с целочисленными разностными коэффициентами различных порядков разности обеспечивает замену аппаратнозатратных операций умножения алгоритмическими операциями сложения и сдвига цифровых отсчетов обрабатываемых сигналов [4-5].

Концепция дедуктивной обработки цифровых сигналов от измерительного прибора представляет собой совокупность принципов обработки таких сигналов на основе численных методов без использования аппаратнозатратных операций умножения. Эта концепция состоит в применении методов построения рекуррентных алгоритмов преобразования и частотной селекции цифровых сигналов от измерительного прибора только алгоритмическими операциями сложения и сдвига разностных отсчетов этих сигналов. Основными принципами этой концепции являются использование метода конечных разностей и применение тривиальных или бинарных разностных отсчетов цифровых сигналов и коэффициентов их разностной цифровой фильтрации и частотного сдвига.

Дедуктивная обработка цифрового сигнала предполагает, что на основе теоретических моделей и алгоритмов цифровой обработки сигналов разрабатываются практические решения задач цифровой обработки сигнала для дедуктивных подходов к его обработке.

Дедуктивные подходы к цифровой обработке сигналов – это методология, на базе которой сложные задачи решаются через последовательное применение простых математических моделей и алгоритмов, основанных на свойствах дискретных сигналов и систем. Такие подходы позволяют упростить обработку сложных сигналов, которые являются суперпозицией элементарных сигналов, и обеспечить точность решений за счёт учёта всех аспектов решения задач цифровой обработки сигналов. Реализация дедуктивных подходов к обработке цифрового сигнала включает следующие этапы:

- 1) создание модели сигнала, например, в виде функциональной зависимости;
- 2) анализ свойств сигнала с помощью математических методов, таких, например, как метод конечных разностей;
- 3) применение алгоритмов частотной селекции цифровых сигналов путём разностной цифровой фильтрации, которая позволяет обрабатывать сигналы, учитывая их частотные характеристики, и выделять информационные (полезные) составляющие сигнала и подавлять шумы помехи;
- 4) применение алгоритмов спектрального анализа путём многоступенчатого преобразования Фурье для обработки больших массивов данных.

Сущность дедуктивности обработки цифрового сигнала состоит в том, что физический сигнал преобразуется в последовательность чисел, которая затем подвергается математическим преобразованиям в вычислительном устройстве путем последовательного продвижения от простых моделей к сложным без необходимости перебора всех возможных вариантов, что снижает сложность реализации алгоритмов цифровой обработки сигнала.

Понятие и термин «*дедуктивная обработка цифровых сигналов*» были предложены и определены для определения и обозначения способов, методов и алгоритмов цифровой обработки сигналов с

малоразрядными коэффициентами фильтрации, формируемыми на основе метода конечных разностей и условно именуемыми «разностными коэффициентами», а применены при построении алгоритмов разностной цифровой фильтрации и многоступенчатого дискретного преобразования Фурье [8-17]. Этот термин свидетельствует о применении разностных схем на основе метода конечных разностей для формирования коэффициентов цифровой фильтрации, каждый из которых заменён разностью между ним и соседним коэффициентами, условно именуемой «разностным коэффициентом 1-го порядка разности» и, в свою очередь, замененной разностью между этим и соседним разностным коэффициентом 1-го порядка разности, условно именуемой «разностным коэффициентом 2-го порядка разности» и также замененной разностью между этим и соседним разностным коэффициентом 2-го порядка разности, условно именуемой «разностным коэффициентом 3-го порядка разности», и т.д. [8-9].

В дедуктивной обработке цифровых сигналов используется совокупность методов, которая включает метод конечных разностей, многоступенчатое преобразование Фурье и разностную цифровую фильтрацию. Эти методы применяются для решения задач спектрального анализа, фильтрации и снижения вычислительной сложности алгоритмов.

При дедуктивной обработке цифровых сигналов реализуются:

- частотный перенос полосовых спектров на основе метода CORDIC, позволяющему получать вектор $y(n \cdot T) = \text{Re}[y(n \cdot T)] + i \cdot \text{Im}[y(n \cdot T)]$, $n=0,1,2 \dots N-1$, $T=2 \cdot \pi / \omega_D$, при повороте вектора $x(n \cdot T) = \text{Re}[x(n \cdot T)] + i \cdot \text{Im}[x(n \cdot T)]$, $n=0,1,2 \dots N-1$, $T=2 \cdot \pi / \omega_D$, на угол Θ без выполнения арифметических операций умножения по формулам (1) – (3):

$$\text{Re}[y(n \cdot T)] = -\text{Im}[x(n \cdot T)], \text{Im}[y(n \cdot T)] = +\text{Re}[x(n \cdot T)], \text{ если } \Theta = \pi \cdot 2 \pm 2 \cdot \pi; \quad (1)$$

$$\text{Re}[y(n \cdot T)] = -\text{Re}[x(n \cdot T)], \text{Im}[y(n \cdot T)] = -\text{Im}[x(n \cdot T)], \text{ если } \Theta = \pi \pm 2 \cdot \pi; \quad (2)$$

$$\text{Re}[y(n \cdot T)] = +\text{Im}[x(n \cdot T)], \text{Im}[y(n \cdot T)] = -\text{Re}[x(n \cdot T)], \text{ если } \Theta = 3\pi/2 \pm 2 \cdot \pi; \quad (3)$$

- построение разностных схем с параметрами $x(n \cdot T)$, $y(n \cdot T)$ и $z(n \cdot T)$ при $n=0,1,2 \dots N-1$ и $T=2 \cdot \pi / \omega_D$ на основе метода конечных разностей по формуле (4):

$$z(n \cdot T) = x(n \cdot T) - y(n \cdot T), \quad (4)$$

- оптимальный поиск значений параметра $y(n \cdot T)$ по методу направленного перебора значений параметра $x_p(n \cdot T)$ при $n=0,1,2 \dots N-1$, $T=2 \cdot \pi / \omega_D$, $p=1,2,3 \dots P-2$ по формулам (5) – (7):

$$y(n \cdot T) = x_{p-1}(n \cdot T), x_{p-1}(n \cdot T) < x_p(n \cdot T), x_p(n \cdot T) < x_{p+1}(n \cdot T), p=1,2,3 \dots P-2; \quad (5)$$

$$y(n \cdot T) = x_p(n \cdot T), x_{p-1}(n \cdot T) > x_p(n \cdot T), x_p(n \cdot T) < x_{p+1}(n \cdot T), p=1,2,3 \dots P-2; \quad (6)$$

$$y(n \cdot T) = x_{p+1}(n \cdot T), x_{p-1}(n \cdot T) > x_p(n \cdot T), x_p(n \cdot T) > x_{p+1}(n \cdot T), p=1,2,3 \dots P-2; \quad (7)$$

Для снижения вычислительной сложности выделения гармонических составляющих $\{x_m(n \cdot T)\}$, $m=0,1,2 \dots N-1$, комплексного сигнала $\{x(n \cdot T)\}$, $n=0,1,2 \dots N-1$, $T=2 \cdot \pi / \omega_D$, применены следующие принципы снижения вычислительной сложности при построении цифровых алгоритмов дедуктивной обработки цифровых сигналов за счет использования только алгоритмических операций наименьшей вычислительной сложности:

- принцип «конечных разностей» отсчётов временной выборки цифрового сигнала по формуле (8):

$$\Delta_x[x(n+1)] = x(n+1) - x(n), \quad (8)$$

где Δ_x – «разрядный оператор», который сопоставляет функцию $x(n)$ с функцией $\Delta_x[x(n+1)]$, определяемой как «конечная разность» отсчётов временной выборки цифрового сигнала;

$x(n)$ – n -ый отсчёт временной выборки цифрового сигнала N -ой длины;

$\Delta_x[x(n+1)]$ – «конечная разность» $(n+1)$ -го и n -го отсчётов цифрового сигнала;

N – длина временной выборки цифрового сигнала.

- принцип «конечных разностей» отсчётов импульсной характеристики цифровой фильтрации по формуле (9):

где Δ_h – «разрядный оператор», который сопоставляет функцию $h(k)$ с функцией $\Delta_h[h(k+1)]$, определяемой как «конечная разность» отсчётов импульсной характеристики цифровой фильтрации K -го порядка $\{h(k)\}$ при $k=0,1,2 \dots K-1$;

$h(k)$ – k -ый отсчёт импульсной характеристики цифровой фильтрации K -го порядка;

$\Delta_h[h(k+1)]$ – «конечная разность» $(k+1)$ -го и k -го отсчётов импульсной характеристики цифровой фильтрации K -го порядка;

$$\Delta_h[h(k+1)] = h(k+1) - h(k), \quad (9)$$

K – число отсчётов импульсной характеристики цифровой фильтрации.

– принцип разделения частотного спектра $\{X(m_l \cdot \Omega_l)\}$, $m_l=0,1,2 \dots M_l-1$, $\Omega_l=\omega_D/(2 \cdot M_l)$, $l=1,2,3 \dots L$, N -точечного фрагмента временной выборки $\{x(n \cdot T)\}$, $n=0,1,2 \dots N-1$, $T=2 \cdot \pi/\omega_D$, на M_l узкополосных спектральных компонентов $\{x(m_l \cdot \Omega_l, n_l \cdot T_l)\}$, $m_l=0,1,2 \dots M_l-1$, $\Omega_l=\omega_D/(2 \cdot M_l)$, $n_l=0,1,2 \dots N/M_l-1$, $T_l=2 \cdot \pi \cdot M_l/\omega_D$, при $M_l \leq N$, $l=1,2,3 \dots L$, и их частотного сдвига без выполнения арифметических операций умножения;

– принцип низкочастотной разностной цифровой фильтрации с k_J -ми разностными коэффициентами K_P -го порядка и J -го порядка разности $h_p(J, k_J)$, $k_J=0,1,2 \dots K_P-1$ комплексного сигнала $\{x(n \cdot T)\}$, $n=0,1,2 \dots N-1$, $T=2 \cdot \pi/\omega_D$ по формуле (10) только алгоритмическими операциями сложения и сдвига за счет тривиальности или бинарности целочисленных значений разностных коэффициентов:

$$y(n \cdot T) = \sum_{k_0=0}^{K_P-1} \sum_{k_1=0}^{k_0} \dots \sum_{k_{J-1}=0}^{k_{J-2}} \sum_{k_J=0}^{k_{J-1}} h_p(J, k_J) \times x(n \cdot T - k_J \cdot T), \quad n=0,1,2 \dots N-1, \quad T=2 \cdot \pi/\omega_D, \quad (10)$$

Численные методы и рекурсивные алгоритмы дедуктивной обработки сигналов могут успешно применяться для выделения гармонических составляющих сигналов от цифровых датчиков колебаний при вибродиагностике:

- двигателей внутреннего сгорания наземных транспортных средств [19-20];
- турбореактивных двухконтурных двигателей воздушных судов [18];
- жидкостных ракетных двигателей космических летательных аппаратов [7].

Областями применения дедуктивной обработки сигналов могут стать также следующие научно-технические приложения [4-5]:

- программное обеспечение шумопеленгования в гидроакустике;
- цифровой спектральный анализ в радиотехнике;
- частотная селекция сигналов в электросвязи.

Постоянное развитие элементной базы микроэлектроники стимулирует перспективные разработки вычислительных алгоритмов численных методов преобразования цифровых сигналов элементарными электронными устройствами. В ряде случаев при построении этих алгоритмов можно использовать рекуррентные алгоритмы дедуктивной обработки цифровых сигналов на микроэлектронных устройствах цифровой обработки сигналов (ЦОС).

Частотная селекция цифровых сигналов до сих пор остается базовым инструментарием их дедуктивной обработки [10, 14]. Различные методы цифровой фильтрации и дискретного преобразования Фурье составляют основу этого инструментария [8-17]. Их вычислительные алгоритмы успешно реализуются на цифровых сигнальных процессорах и программируемых логических интегральных схемах (ПЛИС), в которых равенство скоростей выполнения операций умножения и сложения обеспечивается, в основном, аппаратными средствами [21-24].

Поэтому модификация некоторых методов цифровой фильтрации и дискретного преобразования Фурье позволяет снижать аппаратные затраты на программно-аппаратную реализацию цифровых алгоритмов спектрального анализа за счет уменьшения в них требуемого числа алгоритмических операций умножения, если использовать разностные схемы на основе метода конечных разностей [1-5].

Достоверность результатов исследования обеспечивается применением численных методов математического моделирования и подтверждается соответствием основным принципам построения цифровых фильтров [1-3, 8-9, 15, 17].

Заключение

Предложенная концепция дедуктивной обработки цифровых сигналов без аппаратнозатратных операций умножения определяет и предусматривает возможность снижения вычислительной сложности цифровых алгоритмов обработки сигналов за счёт применения численных методов сведения прямых вычислений сложных функций к выполнению простых операций сложения и сдвига. Для снижения вычислительной сложности алгоритмов цифровой обработки сигналов для выделения гармонических составляющих полигармонического сигнала на фоне случайной помехи с равномерно распределённой спектральной плотностью мощности применены принципы разделения его частотного спектра на узкополосные спектральные компоненты, частотного сдвига этих компонентов и их низкочастотной разностной цифровой фильтрации с целочисленными разностными коэффициентами различных порядков разности без выполнения алгоритмических операций умножения.

Поэтому, численные методы и рекуррентные алгоритмы дедуктивной обработки цифровых сигналов без аппаратнозатратных операций умножения могут быть использованы при преобразовании и обработке цифровых сигналов от измерительных приборов и при цифровизации перспективных методов

преобразования и обработки результатов измерений и контроля с использованием минимального объема аппаратных средств умножения частотно-временных отсчетов обрабатываемых сигналов и амплитудно-частотных характеристик цифровых фильтров.

Численные методы и рекуррентные алгоритмы дедуктивной обработки цифровых сигналов успешно реализуются на ПЛИС, в которых практическое равенство таких процедур программного обеспечения как процедура сложения и процедура умножения реализуются за счет аппаратно-программного обеспечения. В условиях острого дефицита интегральных микросхем в развитых и развивающихся странах по всему миру применение методов и алгоритмов дедуктивной обработки цифровых сигналов позволит экономить аппаратные средства на выполнение цифровой обработки сигналов.

Литература

1. Rabiner L.R., Rader C.M. Digital Signal Processing. – New York: IEEE Press, 1972. – 528 p.
2. Oppenheim A.V., Schaffer R.W. Digital Signal Processing. – Englewood Cliffs, New York: Prentice-Hall, 1975. – 585 p.
3. Rabiner L.R., Gold B. Theory and Application of Digital Signal Processing. – Englewood Cliffs: Prentice-Hall, 1975. – 762 p.
4. Буров Ю.Я., Бурова А.Ю. Дедуктивная обработка цифровых сигналов на основе метода конечных разностей и методов разностной цифровой фильтрации и многоступенчатого дискретного преобразования Фурье, не требующего выполнения арифметических операций умножения // Российское научно-техническое общество радиотехники, электроники и связи имени А.С.Попова: 65 Научная сессия, посвященная Дню радио: доклады. – М.: РНТОРЭС, 2010. – С.425-428.
5. Burova A.Yu. Digital signal processing without performing arithmetic multiplication operations // Amazonia Investiga, 2020. – Vol. 9, № 25. – Pp.200-205.
6. Бурова А.Ю. Анэррорика дедуктивной обработки цифровых сигналов на основе их многоступенчатого дискретного преобразования Фурье // XXII Международная конференция «Цифровая обработка сигналов и ее применение DSPA-2020», 25 марта – 27 марта 2020 г., Москва, Россия: Доклады. – С. 513–518.
7. Kochetkov Y.M., Burova A.Y. Unerroric of engine vibration control by digital method of Deductive signal processing // Smart Innovation, Systems and Technologies, 2022. – Vol. 275. – Pp. 869-874. – DOI: https://doi.org/10.1007/978-981-16-8829-4_85.
8. Шинаков Ю.С., Буров Ю.Я. Разностная цифровая фильтрация с целочисленными коэффициентами // I-я Международная конференция: «Цифровая обработка сигналов и её применения», 30 июня – 3 июля 1998 г., Москва, Россия: Доклады: Том II. – М.: МЦНТИ, 1998. – С.94-99.
9. Шинаков Ю.С., Буров Ю.Я., Бурова А.Ю. Теория, методы и алгоритмы разностной цифровой фильтрации // 3-я Международная конференция: «Цифровая обработка сигналов и её применение», 29 ноября – 1 декабря 2000 г., Москва, Россия: Доклады: Том 1. – М.: МЦНТИ, 2000. – С.96-99.
10. Burova A.Yu., Usatenko T.O. Digital Algorithms for the Discrete Frequency Selection of Signals that Do Not Use Algorithmic Multiplication Operations // TEM Journal, 2020. – Vol. 9, Issue 2. – Pp. 501-506. – DOI: <https://doi.org/10.18421/TEM92-11>.
11. Burova A.Yu., Ryapukhin A.V., Muntyan A.R. Reduced hardware costs with software and hardware implementation of digital methods multistage discrete Fourier transform on programmable logic devices // Amazonia Investiga, 2020. – Vol. 9, Issue 27. – Pp. 227–233.
12. Burova A.Yu. Concept of multistage discrete Fourier transform without performing multiplications // Journal of Physics: Conference Series, 2021, 1889(2), 022003. – DOI: <https://doi.org/10.1088/1742-6596/1889/2/022003>.
13. Burova A.Yu., Ryapukhin A.V. Reduction of the number of multiplication operations in digital signal processing algorithms by classical methods of discrete Fourier transform // AIP Conf. Proc. 2402, 040002 (2021). – DOI: <https://doi.org/10.1063/5.0071449>.

14. Burova A.Yu., Usatenko T.O. Digital methods of discrete Fourier transform, allowing minimizing the number of algorithmic multiplication operations // Journal of Physics: Conference Series. II International Scientific Conference on Metrological Support of Innovative Technologies (ICMSIT II-2021). – Krasnoyarsk, 2021. – DOI: <https://doi.org/10.1088/1742-6596/1889/3/032035>.
15. Arapov N.V., Burova A.Y. Accuracy of Spectral Analysis Based on Difference Digital Filtering // 24th International Conference on Digital Signal Processing and its Applications, DSPA-2022. – Moscow, 2022. – DOI: <https://doi.org/10.1109/DSPA53304.2022.9790761>.
16. Бурова А.Ю. Теория и методология многоступенчатого дискретного преобразования Фурье без использования операций умножения. – М.: Доброе слово и Ко, 2023. – 281 с.
17. Зинченко А.С., Бурова А.Ю. Численные методы программного моделирования цифровых алгоритмов разностной фильтрации без алгоритмических операций умножения // Успехи современной радиоэлектроники, 2025. – Т. 79, № 7. – С. 48-61.
18. Мышелов Е.П., Бурова А.Ю. Цифровизация контроля качества работы авиадвигателей // Контроль качества продукции, 2021. – №11. – С. 40-41.
19. Burova A.Yu., Kabakov V.V. Automatic control of working car engine vibrations using multi-stage discrete Fourier transformation // Journal of Physics: Conference Series, 2020. – Vol. 1679(2). – Pp. 022025. – DOI: <https://doi.org/10.1088/1742-6596/1679/2/022025>.
20. Burova A.Y., Mamonov V.A., Bulychiev N.A. Unerronic of vibration diagnostics of a hydrogen engine // International Journal of Hydrogen Energy, 2024. – Vol. 51. – Pp. 87-95. – DOI: <https://doi.org/10.1016/j.ijhydene.2023.09.129>.
21. Витязев В.В., Витязев С.В., Харин А.В. Многоядерные цифровые сигнальные процессоры платформы TMS320C66xx : учебное пособие. – Рязань: РГРТУ, 2014. – 181 с.
22. Стещенко В.Б. ПЛИС фирмы «ALTERA». Элементная база, система проектирования и языки описания аппаратуры. – М.: ДМК Пресс, 2016. – 576 с.
23. Витязев С.В. Цифровые процессоры обработки сигналов. Курс лекций : учебное пособие. – М.: Горячая линия - Телеком, 2019. – 100 с.
24. Косичкина Т.П., Сперанский В.С. Цифровые сигнальные процессоры и их применение в системах телекоммуникаций и электроники. – М.: Горячая линия - Телеком, 2022. – 315 с.

THEORETICAL FOUNDATIONS AND CONCEPT OF DEDUCTIVE DIGITAL SIGNAL PROCESSING

Eng. Burov Yu.Ya.¹, Lect. Burova A.Yu.²,

¹Russian Scientific and Technical Society of Radio Engineering, Electronics and Communications named after A.S. Popov,

²Moscow Aviation Institute (National Research University),

The article discusses the possibilities of digitalizing measurement and control algorithms without using multiplication operations. The relevance of this research is due to the different hardware requirements of digital implementations of various arithmetic operations that are necessary for signal transformation. The goal of the study is to develop a concept for their deductive digital processing. The study uses mathematical and software modeling methods for digital signals and algorithms. The results of the study demonstrate the advantages of deductive processing of such signals. A concept for this processing has been developed and described. The theoretical foundations of this digital processing and the areas of application of its algorithms for processing measurement and control results have been determined



ВРЕМЕННОЙ РЯД ОШИБОК АДАПТИВНОГО ЭКВАЛАЙЗЕРА: ДЕКОМПОЗИЦИЯ НА ТРЕНД И ОСТАТОК В КОНТЕКСТЕ РОБАСТНОЙ ФИЛЬТРАЦИИ

к.т.н. Мокринский Д.В., д.т.н. Тоискин В.Е.

Филиал Военной академии Ракетных войск Стратегического назначения им. Петра

Настоящая работа посвящена исследованию последовательности ошибок адаптивного эквалайзера как временного ряда в контексте обработки радиосигналов. Рассматриваются особенности формирования последовательности ошибок при адаптации фильтра с использованием обучающей последовательности, выделяются переходной и установившийся режимы. Показано, что переходной процесс может быть представлен как временной ряд с явно выраженным трендом и стохастическим остатком. Проанализированы параметрические, непараметрические и полупараметрические подходы к моделированию тренда и остатка. Особое внимание уделяется проблеме выбора порога функции влияния в робастных адаптивных алгоритмах с учетом текущего значения тренда. Обоснована необходимость разработки робастных адаптивных методов с адаптивным порогом или адаптивной функцией влияния, учитывающих специфику переходного процесса

1. Введение

Адаптивная обработка сигналов с использованием адаптивных фильтров представляет собой одно из фундаментальных направлений современной цифровой обработки сигналов. Адаптивные фильтры находят широкое применение в различных областях: от подавления шума и акустического эха до идентификации систем и выравнивания каналов связи [1-3]. Особую актуальность адаптивные эквалайзеры приобретают в системах декаметрового (ДКМВ) радиосвязи. ДКМВ-радиосвязь использует ионосферу в качестве отражающей среды, что обеспечивает возможность связи на большие расстояния при относительно низком энергопотреблении. Однако ионосферный канал характеризуется рядом существенных недостатков: многолучевым распространением сигнала, селективными замираниями, доплеровским рассеянием и быстрой временной изменчивостью параметров канала [4-5]. Эти факторы приводят к возникновению межсимвольной интерференции, которая значительно ухудшает качество приема цифровых сигналов.

Для компенсации искажений, вносимых каналом связи, на приемной стороне используются адаптивные эквалайзеры, которые непрерывно подстраивают свои коэффициенты в соответствии с изменяющимися характеристиками канала [2]. Типичный режим работы адаптивного эквалайзера включает две фазы: фаза обучения, во время которой передается известная обучающая последовательность, на основе которой настраиваются весовые коэффициенты адаптивного фильтра; фаза работы во время которой осуществляется обработка информационной последовательности с фиксированными весовыми коэффициентами, полученными на этапе обучения.

Наиболее широко применяемыми алгоритмами адаптации являются алгоритм наименьших средних квадратов (LMS, Least Mean Squares) и рекурсивный алгоритм наименьших квадратов (RLS, Recursive Least Squares) [1-2]. Эти алгоритмы обеспечивают компромисс между вычислительной сложностью и скоростью сходимости.

Важным аспектом функционирования адаптивного эквалайзера является анализ последовательности ошибок, формирующейся в процессе адаптации. Ошибка представляет собой разность между выходным сигналом фильтра и эталонной (обучающей) последовательностью. Изучение статистических свойств этой последовательности позволяет глубже понять механизмы сходимости адаптивных алгоритмов и разработать более эффективные робастные методы адаптации.

Целью настоящей работы является рассмотрение последовательности ошибок адаптивного эквалайзера как временного ряда, выделение в нем тренда и стохастического остатка, а также обоснование необходимости учета характера тренда при проектировании робастных адаптивных алгоритмов.

2. Специфика формирования последовательности ошибок во время обучения адаптивного эквалайзера.

Адаптивный эквалайзер представляет собой цифровой фильтр с настраиваемыми весовыми коэффициентами, предназначенный для компенсации искажений, вносимых каналом связи. Обозначим через

$$w(n) = [w_0(n), w_1(n-1), \dots, w_m(n-m+1)]^T$$

вектор весовых коэффициентов фильтра длины M в момент времени n .

Входной сигнал эквалайзера представляет собой вектор

$$x(n) = [x(n), x(n-1), \dots, x(n-m+1)]^T,$$

где $x(n)$ – отсчет принятого сигнала. Выходной сигнал фильтра определяется соотношением:

$$y(n) = \mathbf{w}^T(n)\mathbf{x}(n) = \sum_{k=0}^{M-1} w_k(n)x(n-k). \quad (1)$$

В режиме обучения используется известная обучающая последовательность $d(n)$, которая соответствует переданным символам. Сигнал ошибки определяется как:

$$e(n) = d(n) - y(n) = d(n) - \mathbf{w}^T(n)\mathbf{x}(n) \quad (2)$$

После обработки обучающей последовательности длиной N_{train} вектор весовых коэффициентов фиксируется, и эквалайзер переходит в режим обработки информационной последовательности длиной N_{data} . Таким образом, полный цикл работы эквалайзера включает:

$$N_{total} = N_{train} + N_{data} \quad (3)$$

В условиях нестационарного канала связи, характерного для ДКМВ-радиосвязи, параметры канала изменяются во времени. По завершении обработки информационной последовательности необходимо очередное обучение эквалайзера. Таким образом, процесс адаптации носит периодический и разрывный характер: после каждой информационной последовательности переходной процесс возобновляется заново.

В дальнейшем значения ошибки используются для итерационного процесса поиска минимума функции ошибки и соответствующего ей вектора весовых коэффициентов. В зависимости от используемого алгоритма уравнение обновления вектора весовых коэффициентов может иметь различный вид.

Например, для LMS:

$$\mathbf{w}(n+1) = \mathbf{w}(n) + \mu \mathbf{x}(n)e(n), \quad (4)$$

где μ – параметр размера шага, определяющий скорость адаптации и устойчивость алгоритма; для RLS

$$\begin{aligned} \mathbf{k}(n) &= \frac{\lambda^{-1} \mathbf{P}(n-1)\mathbf{x}(n)}{1 + \lambda^{-1} \mathbf{x}^H(n) \mathbf{P}(n-1)\mathbf{x}(n)}, \\ e(n) &= d(n) - \mathbf{w}^T(n-1)\mathbf{x}(n), \\ \mathbf{w}(n) &= \mathbf{w}(n-1) + \mathbf{k}(n)e(n), \\ \mathbf{P}(n) &= \lambda^{-1} \mathbf{P}(n-1) - \lambda^{-1} \mathbf{k}(n)\mathbf{x}^H(n) \mathbf{P}(n-1), \end{aligned} \quad (5)$$

где $\mathbf{k}(n)$ – вектор коэффициентов усиления, $\mathbf{P}(n)$ – матрица обратной корреляции входных данных.

Последовательность ошибок, формирующаяся в результате процессов (4, 5) $\{e(n), n=1, 2, \dots, N_{train}\}$ может быть условно разделена на две фазы:

1. Переходной процесс - на начальном этапе адаптации ошибка имеет значительную величину и демонстрирует нисходящую тенденцию по мере настройки весовых коэффициентов. Длительность переходного процесса зависит от свойств входного сигнала, параметров алгоритма адаптации и начальных условий.

2. Установившийся режим - после завершения переходного процесса ошибка колеблется около нуля с относительно малой амплитудой. В установившемся режиме средняя квадратичная ошибка (MSE) достигает некоторого минимального значения.

Формально можно записать:

$$e(n) = \begin{cases} e_{trans}(n), & n \leq n_{trans}, \\ e_{ss}(n), & n > n_{trans}, \end{cases} \quad (6)$$

где n_{trans} – момент перехода в установившийся режим, $e_{trans}(n)$ – ошибка в переходном процессе, $e_{ss}(n)$ – ошибка в установившемся режиме.

3. Представление переходного процесса как временного ряда

Последовательность ошибок в переходном процессе $\{e_{trans}(n), n=1, 2, \dots, n_{trans}\}$ может быть рассмотрена как временной ряд. Ключевым свойством этого временного ряда [5,6] является наличие существенной корреляции между последовательными значениями, обусловленной инерционностью процесса адаптации. Применяя классическую декомпозицию временных рядов, можно представить ошибку переходного процесса в виде:

$$e_{trans}(n) = T(n) + \varepsilon(n), \quad (7)$$

где $T(n)$ – детерминированная или слабо стохастическая компонента тренда, $\varepsilon(n)$ – стохастический остаток или шумовая составляющая.

Характер тренда зависит от используемого алгоритма адаптации, свойств входного сигнала и параметров настройки. В литературе предложено несколько моделей для описания тренда переходного процесса адаптивных фильтров.

Для алгоритма LMS при предположении о белом гауссовском входном сигнале и малом параметре шага μ среднеквадратичная ошибка в переходном процессе может быть аппроксимирована экспоненциальной функцией [2,7]:

$$E[e^2(n)] \approx \sigma_e^2 + c \cdot \exp(-an), \quad (8)$$

где σ_e^2 – дисперсия остатка в установившемся режиме, C – константа, зависящая от начальных условий, a – константа скорости сходимости, связанная с параметром шага μ и собственными значениями корреляционной матрицы входного сигнала.

Следовательно, для ошибки можно записать:

$$T(n) = |e_{trans}| \approx \sqrt{\sigma_e^2 + c \cdot \exp(-an)} \approx A_0 \cdot \exp(-\beta n) + B, \quad (9)$$

где A_0, β, B – параметры модели.

При более точном анализе, учитывающем различные моды сходимости, связанные с собственными значениями корреляционной матрицы, тренд может быть представлен в виде суммы экспонент [8,9]:

$$T(n) = \sum_{i=1}^K A_i \exp(-\beta_i n) + B \quad (10)$$

где K – число мод, A_i, B_i – параметры, связанные с i -ой модой.

В некоторых работах предлагаются и другие функции для описания тренда, такие как степенные функции, гиперболические зависимости и их комбинации [10,11]. Выбор конкретной модели зависит от условий применения и требуемой точности аппроксимации.

Параметр, характеризующий начальное значение ошибки

$$e(1) = d(1) - w^T(1)x(1) \quad (11)$$

зависит от начального вектора весовых коэффициентов $w(1)$ и первого входного вектора $x(1)$. Обычно начальный вектор весов устанавливается равным нулю или некоторому случайному значению. Входной вектор $x(1)$ является реализацией случайного процесса, зависящей от переданных символов и характеристик канала. Следовательно, начальная величина ошибки $e(1)$ также представляет собой случайную величину. Следовательно, параметр A_0 в экспоненциальной модели является случайной величиной:

$$A_0 \square p_{A_0}(a), \quad (12)$$

где P_{A_0} – плотность распределения вероятности начального значения тренда.

Кроме того, аналогичными свойствами обладает первое значение ошибки очередной обучающей последовательности, в данном случае состояние вектора весов определяется циклом предыдущего обучения.

Оценка того, каким законом распределения можно аппроксимировать параметр A_0 является исследовательской задачей.

Скорость сходимости зависит от параметра шага и собственных значений корреляционной матрицы входного сигнала R_x . В случае коррелированного входного сигнала собственные значения определяют динамику сходимости:

$$\beta_i = \mu \lambda_i. \quad (13)$$

Поскольку корреляционная матрица R_x зависит от статистических свойств входного сигнала, которые могут изменяться от одного сеанса связи к другому, скорость сходимости также является случайной величиной:

$$\beta \square p_\beta(b), \quad (14)$$

В условиях нестационарного канала изменения импульсной характеристики канала приводят к вариациям R_x во времени, что дополнительно увеличивает стохастичность параметра β .

4. Особенности представления переходного процесса адаптивного эквалайзера как временного ряда при использовании робастных алгоритмов адаптивной фильтрации.

Робастные адаптивные алгоритмы, основанные на М-оценках, предназначены для подавления влияния выбросов в данных, вызванных импульсным шумом или другими аномалиями [12, 13]. В таких алгоритмах сигнал ошибки модифицируется через функцию влияния $\psi(\cdot)$:

$$w(n) = w(n-1) + \Gamma \cdot \psi(e(n)), \quad (15)$$

где Γ – оператор характеризующий конкретный способ адаптивной фильтрации, а функция $\psi(\cdot)$ ограничивает или обрезает большие значения ошибок.

Общеизвестными функциями влияния являются: Функция Хьюбера, Функция Хэмпеля, Функция Тьюки и др [12, 13]. Кроме того часто используются их модифицированные версии с адаптацией параметров.

Применение функции влияния $\psi(\cdot)$ существенно изменяет динамику сходимости алгоритма. Тренд ошибки для робастных алгоритмов становится сложнее для аналитического описания по следующим причинам:

- функция $\psi(\cdot)$ вносит нелинейность в процесс обновления весов, что усложняет аналитическое решение;
- параметр порога в кусочно-заданных функциях влияет на характер тренда, определяя, какие ошибки будут обрезаны.

Несмотря на сложность аналитического описания, можно выделить общие характеристики тренда для робастных алгоритмов.

1. Начальное значение $T(1)$ и начальное значение в начале каждой очередной обучающей последовательности $T(i)$, а также коэффициент сходимости β являются случайными величинами, зависящие от начальных условий, свойств входного сигнала, длин обучающей и информационной частей обрабатываемых пакетов, используемого адаптивного алгоритма и характеристик канала связи.

2. Математическое ожидание тренда $E(T(n))$ является убывающей функцией времени (n) то есть имеет нисходящий характер:

$$E\left(\frac{dT(n)}{dn}\right) < 0, n \in [1, n_{trans}].$$

3. Асимптотическое поведение:

$$\lim_{n \rightarrow \infty} T(n) = C, \quad (16)$$

то есть тренд стремится либо к нулю, либо к минимальной дисперсии.

4. Функцию $T(n)$ можно считать гладкой и в частных случаях описывать аналитическими функциями вида 9, 10.

5. Так как функция имеет нисходящий характер, то существует возможность измерить среднее время, за которое тренд уменьшается в определённое количество раз.

Остаток $\varepsilon(n)$ представляет собой стохастическую компоненту ошибки, оставшуюся после удаления тренда. В простейшем случае остаток моделируется как белый гауссовский шум. Параметрическая модель остатка предполагает, что его статистические свойства полностью определяются конечным набором параметров.

Однако для реальных каналов связи, особенно ДКМВ-каналов, остаток может иметь более сложную структуру. В частности, остаток может обладать автокорреляцией:

$$E[\varepsilon(n)\varepsilon(n+k)] \neq 0, k \neq 0 \quad (17)$$

или описываться негауссовскими распределениями (в присутствии импульсных помех остаток может иметь распределение с тяжелыми хвостами, например, α -устойчивое распределение или смесь нормальных распределений [14] и др.).

Для каналов со сложными условиями распространения остатки могут быть описаны в рамках непараметрической модели, которая не налагает жестких предположений о виде распределения. Вместо этого используются методы, основанные на эмпирических данных, такие как: ядерные оценки плотности, в которых плотность распределения оценивается по наблюдениям без предположения о конкретном параметрическом семействе распределений или отдельные робастные статистические оценки в которых используются оценки, устойчивые к выбросам, такие как медиана, усеченное среднее и др. Непараметрические методы обладают большей гибкостью и позволяют адаптироваться к более сложным и разнообразным условиям распространения радиосигнала.

Также на основе вышесказанного можно выделить полупараметрическую модель.

Полупараметрическая модель представляет собой комбинацию параметрического и непараметрического подходов. В контексте анализа последовательности ошибок адаптивного эквалайзера полупараметрическая модель может иметь вид:

$$e_{trans}(n) = T(n; \theta) + \varepsilon(n) \quad (18)$$

где тренд $T(n; \theta)$ задается параметрической функцией с вектором параметров θ (например, экспоненциальной функцией), а остаток $\varepsilon(n)$ моделируется непараметрически.

Полупараметрические модели могут быть актуальны для робастных алгоритмов, где тренд может быть сложным, но его общий характер известен, а остаток может иметь нестандартное распределение из-за сложных условий распространения.

5. Проблема выбора порога с учетом тренда для робастных адаптивных методов, использующих кусочно-заданную функцию влияния

Как было отмечено выше в рамках итерационного обновления вектора весовых коэффициентов (15) чаще всего используют кусочно-заданную функцию $\psi(\cdot)$, например функция Хьюбера (Huber)[12]:

$$\psi_{\text{Huber}}(e) = \begin{cases} e, & |e| \leq \delta, \\ \delta \cdot \text{sgn}(e), & |e| > \delta, \end{cases} \quad (19)$$

Параметр δ называется порогом обрезания и играет критическую роль в работе семейства робастных алгоритмов с кусочно-заданными функциями влияния. При использовании δ заданного в виде константы, если порог δ выбран недостаточно большим по сравнению с текущим значением тренда $|T(n)|$, то систематически будет происходить обрезание ошибки даже в отсутствие выбросов:

$$|e(n)| = |T(n) + \varepsilon(n)| > \delta, \quad (20)$$

это может привести к тому, что обрезание ошибки уменьшает эффективную величину сигнала ошибки, используемого для обновления весов, что замедляет процесс адаптации; систематическое обрезание может привести к смещению весовых коэффициентов относительно оптимальных значений в связи с чем установившееся значение среднеквадратичной ошибки может оказаться выше, чем при использовании не робастного алгоритма. С другой стороны, если порог δ выбран слишком большим, робастный алгоритм теряет свою способность подавлять выбросы, и его поведение приближается к поведению не робастного алгоритма.

Учитывая зависимость оптимального порога от текущего значения тренда, целесообразно применять адаптивный порог $\delta(n)$, изменяющийся во времени в соответствии с динамикой переходного процесса:

$$\delta(n) = f(T(n), \sigma_\varepsilon(n)), \quad (21)$$

где $f(\cdot)$ – некоторая функция, учитывающая величину тренда $T(n)$ и оценку дисперсии остатка $\sigma_\varepsilon(n)$.

Один из подходов к определению адаптивного порога основан на робастной оценке масштаба ошибки. Наиболее распространенным методом является использование медианного абсолютного отклонения (MAD, Median Absolute Deviation) [15]:

$$\hat{\sigma}(n) = \text{median}(|e(n-k) - \text{median}(e(n-k))|) \cdot 1.4826, \quad (22)$$

где медиана вычисляется по скользящему окну наблюдений.

Порог может быть установлен как:

$$\delta(n) = c \cdot \hat{\sigma}(n), \quad (23)$$

где c – коэффициент, выбираемый на основе желаемой вероятности ложного обнаружения выбросов.

Альтернативный подход заключается в использовании адаптивной функции влияния $\psi(e, n)$, параметры которой изменяются во времени:

$$\psi(e, n) = \psi\left(\frac{e - T(n)}{\sigma_\varepsilon(n)}\right), \quad (24)$$

где $T(n)$ – оценка тренда, $\sigma(n)$ – оценка стандартного отклонения остатка.

Такой подход позволяет центрировать и масштабировать ошибку перед применением функции влияния, что обеспечивает корректную работу робастного алгоритма на всех этапах переходного процесса.

В установившемся режиме тренд практически отсутствует, и ошибка определяется только остатком. В этих условиях выбор порога упрощается, так как нет необходимости учитывать значительную детерминированную компоненту. Классические робастные алгоритмы с фиксированным порогом, основанным на оценке дисперсии остатка, эффективно работают в установившемся режиме. На основе вышесказанного можно сделать вывод о том, что различие между переходным и установившимся режимами требует различных стратегий выбора порога.

6. Заключение

В настоящей работе рассмотрена последовательность ошибок адаптивного эквалайзера как временной ряд, что позволило выявить важные закономерности, влияющие на эффективность робастных адаптивных алгоритмов.

Последовательность ошибок в переходном процессе адаптивного эквалайзера может быть представлена в виде суммы детерминированной или слабо стохастической компоненты тренда $T(n)$ и стохастического остатка $\varepsilon(n)$. Тренд отражает динамику сходимости алгоритма адаптации и может быть аппроксимирован различными функциями (экспоненциальными, суммой экспонент и др.), параметры которых являются случайными величинами, зависящими от начальных условий и свойств входного сигнала.

Для робастных алгоритмов, основанных на М-оценках, тренд имеет более сложный характер, затрудняющий его аналитическое описание, однако можно выделить общие характеристики, применимые для широкого класса алгоритмов. Характер тренда критически важен для выбора порога обрезания функции влияния: фиксированный порог, оптимальный для установившегося режима, может привести к систематическому обрезанию ошибок в переходном процессе, что замедляет сходимость и ухудшает качество оценивания. В установившемся режиме влияние тренда отсутствует, и работают классические робастные алгоритмы с порогом, определяемым дисперсией остатка.

Полупараметрические модели, в которых тренд задается параметрически, а остаток – непараметрически, представляют собой перспективный подход для анализа и проектирования робастных адаптивных алгоритмов.

Литература

1. Haykin, S. (2002). Adaptive Filter Theory (4th ed.). Prentice Hall.
2. Widrow, B., & Stearns, S. D. (1985). Adaptive Signal Processing. Prentice Hall.
3. Джиган, В. И. История, теория и практика адаптивной обработки сигналов / В. И. Джиган // Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС). – 2012. – № 1. – С. 30-37.
4. Goodman, J. M., & Aarons, J. (1990). Ionospheric effects on modern electronic systems. Proceedings of the IEEE, 78(3), 512-528.
5. Газизов, Д. И. Обзор методов статистического анализа временных рядов и проблемы, возникающие при анализе нестационарных временных рядов / Д. И. Газизов // Научный журнал. – 2016. – № 3(4). – С. 9-14. – EDN VOXCJZ.
6. Сурина А.В. Анализ временных рядов: Учеб. пособие. СПб., 2025 – 90 с.
7. R. L. Kosut, B. D. O. Anderson, Convergence Properties of Adaptive Systems and the Definition of Exponential Stability, IEEE Trans. Information Theory, 2015
8. T. L. H. Li, C. L. Nikias, “On exact convergence results of adaptive filters: the finite alphabet case”, Signal Processing, vol. 80, no. 7, 2000, pp. 1309–1332.
9. Sayed A. H., “Transient analysis of adaptive filters”, Proc. IEEE ICASSP 2001.
10. Eweda, E. (1990). Analysis and design of a signed regressor LMS algorithm for stationary and nonstationary adaptive filtering with correlated Gaussian data. IEEE Transactions on Circuits and Systems, 37(11), 1367-1374.
11. Yousef, N. R., & Sayed, A. H. (2001). Ability of adaptive filters to track carrier offsets and channel nonstationarity. IEEE Transactions on Signal Processing, 50(7), 1533-1544.
12. Huber, P. J., & Ronchetti, E. M. (2009). Robust Statistics (2nd ed.). John Wiley & Sons.
13. Hampel, F. R., Ronchetti, E. M., Rousseeuw, P. J., & Stahel, W. A. (1986). Robust Statistics: The Approach Based on Influence Functions. John Wiley & Sons.
14. Shao, M., & Nikias, C. L. (1993). Signal processing with fractional lower order moments: stable processes and their applications. Proceedings of the IEEE, 81(7), 986-1010.
15. Rousseeuw, P. J., & Croux, C. (1993). Alternatives to the median absolute deviation. Journal of the American Statistical Association, 88(424), 1273-1283.

TIME SERIES OF ADAPTIVE EQUALIZER ERROR: DECOMPOSITION INTO TREND AND RESIDUAL IN THE CONTEXT OF ROBUST FILTERING

Cand. Sci. (Tech.) D.V. Mokrinskiy, Dr. Sci. (Tech.) V.E. Toiskin

Branch of the Military Academy of Strategic Missile Forces named after Peter the Great

This paper investigates the sequence of adaptive equalizer errors as a time series in the context of radio signal processing. The characteristics of the error sequence formation during filter adaptation using a training sequence are examined, distinguishing between the transient and steady-state modes. It is shown that the transient process can be represented as a time series with a pronounced trend and a stochastic residual. Parametric, nonparametric, and semiparametric approaches to trend and residual modeling are analyzed. Particular attention is paid to the problem of selecting the threshold of the influence function in robust adaptive algorithms, taking into account the current trend value. The necessity of developing robust adaptive methods with an adaptive threshold or an adaptive influence function that accounts for the specific nature of the transient process is substantiated.



АЛГОРИТМ ПРЕОБРАЗОВАНИЯ СИГНАЛИЗАЦИЙ SIP И EDSS1

инж прогр.. Шумилов Н.Н.

АО «Омский научно-исследовательский институт приборостроения»

В работе рассмотрены принципы и алгоритмы преобразования сигнальных сообщений между протоколом инициирования сеансов связи SIP, используемым в IP-телефонии, и системой цифровой абонентской сигнализации EDSS1, функционирующей поверх тракта E1 (Primary Rate Interface). Исследованы правила отображения состояний вызова, форматов сообщений и информационных элементов применительно к временным слотам потока 2048 кбит/с. Особое внимание уделено преобразованию кодов причин завершения вызовов и идентификации B-каналов. Приведены таблицы соответствия ключевых сигналов и диаграммы обмена. Сформулированы требования к реализации процедур преобразования в шлюзах сопряжения.

В условиях сосуществования классических телефонных сетей с коммутацией каналов (TDM) и пакетных сетей задача обеспечения взаимодействия сигнализаций не теряет актуальности. Одной из ключевых точек сопряжения является стык между VoIP-сетью и цифровым потоком E1, в котором для управления вызовами задействован протокол EDSS1 в выделенном D-канале (16-й тайм-слот) [1]. Преобразование сообщений между текстовым протоколом SIP (RFC 3261) и бинарно-ориентированным протоколом EDSS1 (ITU-T Q.931) требует формализации правил отображения как синтаксиса, так и семантики управления соединением на уровне тракта E1 [2].

Целью данной работы являлась формализация правил и алгоритмов преобразования сигнализаций SIP и EDSS1 для базового обслуживания вызова и обработки исключительных ситуаций. Для достижения цели решены следующие задачи: проведён анализ форматов сообщений и процедур управления вызовом в протоколах SIP и EDSS1; разработаны правила отображения (mapping) сообщений и информационных элементов; внедрён механизм преобразования кодов причин завершения вызовов (Q.850 ↔ SIP).

Протокол EDSS1, описанный в рекомендациях ITU-T серии Q.930 и Q.931, является канално-ориентированным протоколом, работающим по выделенному D-каналу интерфейсов первичного доступа PRI E1 [2]. В его основе лежит жёсткая последовательность состояний вызова и бинарное кодирование сообщений. В противоположность ему, SIP, стандартизованный в RFC 3261, является текстовым, транзакционно-ориентированным протоколом прикладного уровня, работающим поверх транспортных протоколов UDP или TCP [3]. Различия в архитектуре и форматах этих протоколов порождают нетривиальную задачу отображения не только синтаксиса сообщений, но и семантики процедур управления вызовом.

Центральным элементом алгоритма преобразования является функция отображения (mapping) сообщений и их параметров. При поступлении запроса SIP INVITE со стороны IP-сети процедура преобразования формирует сообщение EDSS1 SETUP для передачи в D-канал потока E1. Номер вызывающего абонента из поля «From» преобразуется в информационный элемент «Calling Party Number». Номер вызываемого абонента из «Request-URI» размещается в «Called Party Number». Критически важным для тракта E1 является формирование элемента «Channel Identification», который однозначно указывает номер тайм-слота (B-канала) в потоке, выделенного для передачи полезной нагрузки. Параметры кодирования речи из тела SDP отображаются в элемент «Bearer Capability» (речь, 3.1 кГц аудио или данные 64 кбит/с) [3].

Логика преобразования ответных сообщений также строго детерминирована. При получении со стороны тракта E1 сообщения CALL PROCEEDING, означающего, что сеть приняла запрос на установление соединения и приступила к его обработке, на сторону SIP направляется временный ответ 100 Trying. Это предотвращает повторную передачу запроса INVITE со стороны SIP-клиента по истечении таймера. Сообщение ALERTING, свидетельствующее о поступлении вызывного сигнала на терминал вызываемого абонента, отображается в SIP-ответ 180 Ringing. Наконец, ответ абонента, фиксируемый на стороне тракта E1 сообщением CONNECT, преобразуется в окончательный SIP-ответ 200 OK, который завершает начальную транзакцию INVITE. Подтверждение приёма этого ответа со стороны SIP-клиента осуществляется запросом ACK, который, в свою очередь, транслируется в сообщение CONNECT ACKNOWLEDGE протокола EDSS1, завершая процедуру установления соединения с точки зрения тракта E1. Последовательность преобразования при успешном установлении соединения по инициативе SIP-абонента и выходе на тракт E1 приведена на рисунке 1.

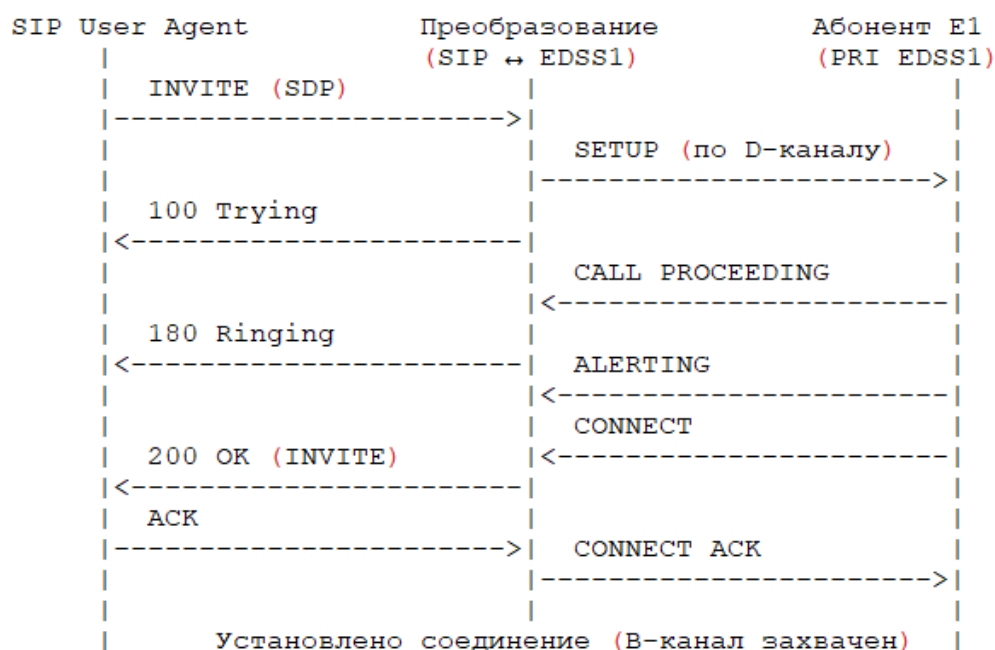


Рисунок 1. Преобразования входящего вызова по инициативе SIP-абонента

При поступлении входящего вызова со стороны тракта E1 (сообщение SETUP в D-канале) алгоритм работает в обратном направлении. На основе номера вызываемого абонента определяется целевой SIP URI и формируется запрос INVITE. Временные ответы SIP отображаются в сигналы CALL PROCEEDING и ALERTING, передаваемые обратно в поток E1, как показано на рисунке 2.

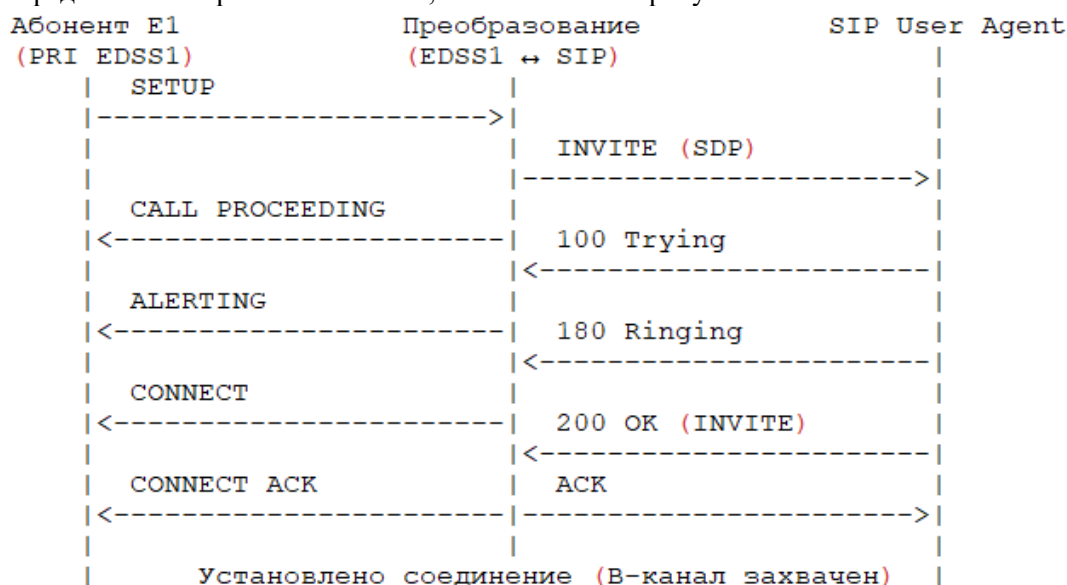


Рисунок 2. Преобразования входящего вызова со по инициативе E1-абонента

Для наглядного представления правил преобразования в таблице 1 представлено соответствие основных сигнальных сообщений.

Таблица 1

Соответствие сигналов SIP и EDSS1 (E1) при установлении соединения

Этап вызова	Протокол SIP	Протокол EDSS1
Инициация вызова	INVITE (с SDP)	SETUP
Подтверждение обработки запроса	100 Trying	CALL PROCEEDING
Оповещение о вызове абонента	180 Ringing	ALERTING
Ответ вызываемого абонента	200 OK (для INVITE)	CONNECT
Подтверждение установления соединения	ACK	CONNECT ACKNOWLEDGE

Процедура разъединения соединения также подчиняется строгим правилам отображения. Запрос завершения вызова SIP BYE преобразуется в сообщение EDSS1 DISCONNECT, передаваемое по D-каналу. В информационном элементе «Cause» указывается код, отображённый из SIP-ответа, либо код нормального разъединения (16). При получении сообщения RELEASE со стороны E1 алгоритм формирует SIP-ответ «200 OK» на запрос BYE. При инициативе отбоя со стороны тракта E1 (сообщение DISCONNECT в потоке) оно преобразуется в запрос BYE в сторону IP-сети.

Критически важной частью алгоритма преобразования является корректное отображение кодов причин завершения вызовов. Протокол EDSS1 использует коды причин, стандартизованные в рекомендации ITU-T Q.850, которые передаются в информационном элементе «Cause» сообщений DISCONNECT и RELEASE. Протокол SIP, в свою очередь, использует числовые коды ответов (от 100 до 699) с текстовыми пояснениями. Для обеспечения информативности для пользователя и корректной работы систем учёта необходимо однозначное соответствие между этими кодами. Правила преобразования для наиболее частотных ситуаций приведены в таблице 2 [4].

Таблица 2

Правила преобразования кодов причин завершения вызова (Q.850 ↔ SIP)

Причина завершения	Код Q.850 (EDSS1)	SIP-ответ
Нормальное разъединение	16	200 OK (BYE)
Абонент занят	17	486 Busy Here
Нет ответа от абонента	19	480 Temporarily Unavailable
Номер не существует / не назначен	1	404 Not Found
Сеть перегружена	42	503 Service Unavailable
Вызов отклонён	21	603 Decline

Для корректной работы с потоком E1 алгоритм преобразования должен отслеживать состояние не только сигнального протокола, но и физического уровня тракта (синхронизация, аварии AIS/LOF). Внутренний конечный автомат должен отображать состояния согласно Q.931 (Null, Call Initiated, Active) на состояния SIP-диалога. Это гарантирует корректное освобождение тайм-слотов при ошибках сигнализации.

Реализация предложенного алгоритма позволяет достичь прозрачного взаимодействия между VoIP-сетями и цифровыми трактами E1 с сигнализацией EDSS1. Перенос обработки состояний на шлюз сопряжения минимизирует задержки и упрощает диагностику. Дальнейшее развитие направления связано с поддержкой дополнительных видов услуг (CLIP, CLIR) и переходом на более широкополосные кодеки в рамках существующей структуры цикла E1.

Литература

1. Программные IP-ATC, E1, DSS-1 и нагрузочное тестирование [Электронный ресурс] // Хабр. – 2020. – URL: <https://habr.com/ru/articles/511158/> (дата обращения 20.04.2026).
2. Kotar P., Gauch F., Pötl J. Interworking between Digital Subscriber Signalling System No. one (DSS1) and Session Initiation Protocol (SIP) for basic call [Электронный ресурс] // Internet-Draft. – 2003. – URL: <https://www.cs.columbia.edu/sip/drafts/sipping/draft-kotar-sipping/dss1/sip-iw-01.txt> (дата обращения 20.04.2026)
3. Vlaovic B., Nedok S., Vicman P., Brezocnik Z. SIP-DSS1 Signalling Gateway [Электронный ресурс] // YUMPU. – URL: <https://www.yumpu.com/en/document/read/36477387/sip-dss1-signalling-gateway-citeeex/5> (дата обращения 20.04.2026)
4. Recommendation ITU-T Q.850: Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISND user part [Электронный ресурс] // ITU-T. – 2018. – URL: <https://www.itu.int/rec/T-REC-Q.850-201810-l/en> (дата обращения 20.04.2026)

SIP AND EDSS1 SIGNALING CONVERSION ALGORITHM

engineer Shumilov N.N.

Omsk Scientific Research Institute of Instrument Engineering

The paper examines the principles and algorithms for converting signaling messages between the Session Initiation Protocol (SIP) and the Euro Digital Subscriber Signalling System No. 1 (EDSS1) operating over an E1 Primary Rate Interface. The rules for mapping call states, message formats, and information elements specific to 2048 kbit/s time slots are investigated. Special attention is paid to the conversion of call termination cause codes and B-channel identification. Tables of correspondence for key signals and sequence diagrams are provided. Requirements for the correct implementation of conversion procedures in gateways are formulated.



СЕКЦИЯ № 4.

**ИНФОРМАЦИОННЫЕ И ИНТЕРНЕТ-ТЕХНОЛОГИИ, В Т.Ч.
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ.**

**ИССЛЕДОВАНИЕ ZERO-SHOT МОДЕЛЕЙ ДЛЯ ПОИСКА РЕПЕРНЫХ ОБЛАСТЕЙ И
УЛУЧШЕНИЯ ПРИВЯЗКИ ИЗОБРАЖЕНИЙ**

доц. Андриянов Н.А.

Финансовый университет при Правительстве Российской Федерации

В работе рассматривается задача поиска реперных областей на изображениях для последующей привязки кадров. На основе Zero-Shot детекторов объектов YOLO-World и Grounding DINO исследуется влияние устойчивости обнаруженных областей на эффективность псевдоградиентной процедуры привязки. Предлагается ансамблевый подход, сочетающий semantic-aware выделение областей и локальные дескрипторы SuperPoint. Исследование выполнено на синтетическом наборе данных объемом 6200 изображений.

Современные методы автоматической привязки изображений опираются на поиск устойчивых локальных признаков и реперных областей, сохраняющих информативность при изменении масштаба, повороте, частичной окклюзии и вариациях освещения. Классические алгоритмы, такие как SIFT и SURF, долгое время являлись базовыми инструментами выделения локальных признаков в задачах фотограмметрии и компьютерного зрения [1, 2]. Несмотря на высокую устойчивость к геометрическим преобразованиям, данные методы работают исключительно на локальных градиентных характеристиках изображения и не используют семантический контекст сцены. Это приводит к тому, что алгоритмы могут выбирать нестабильные или неинформативные области, особенно в условиях сложного фона, шумов и повторяющихся текстур.

Развитие глубоких нейронных сетей привело к появлению архитектур семейства YOLO, ориентированных на быстрое обнаружение объектов в режиме реального времени [3]. Модель YOLO стала одним из наиболее успешных решений благодаря комбинации высокой скорости и точности. Использование CSP-блоков, Mosaic-аугментации, PANet и оптимизированных функций потерь позволило значительно повысить качество детектирования без существенного увеличения вычислительной сложности [4]. В задачах привязки изображений такие модели позволяют перейти от случайного выбора отсчётов к выделению семантически значимых объектов сцены: зданий, мостов, дорожной инфраструктуры, техники и других объектов интереса.

Следующим этапом развития стали open-vocabulary и Zero-Shot модели [5], способные обнаруживать объекты без дополнительного обучения на конкретных классах. Одной из наиболее перспективных архитектур данного типа является YOLO-World [6]. Модель объединяет визуальные признаки изображения с текстовыми эмбедами, формируемыми языковой моделью. Благодаря использованию контрастивного обучения и механизма согласования текстовых и визуальных признаков YOLO-World способна обнаруживать объекты по произвольным текстовым запросам. Это особенно важно в задачах автоматической привязки изображений, где набор объектов интереса заранее неизвестен и может изменяться в зависимости от сценария применения.

Другим современным подходом является Grounding DINO [7], использующий трансформерную архитектуру и мультимодальное обучение. В отличие от классических детекторов, Grounding DINO интегрирует текстовую информацию непосредственно в процесс формирования attention-карт. Это позволяет более точно локализовать объекты и обеспечивает высокую устойчивость к частичной окклюзии и изменению положения объекта в кадре. Однако высокая точность достигается ценой увеличения вычислительных затрат и снижения скорости обработки по сравнению с YOLO-World.

Для повышения устойчивости реперных областей в современных исследованиях активно применяются self-supervised методы выделения локальных признаков. Модель SuperPoint [8] позволяет формировать устойчивые ключевые точки и дескрипторы без необходимости ручной разметки данных. В дальнейшем полученные признаки могут быть сопоставлены при помощи графовых нейронных сетей, например SuperGlue [9], что обеспечивает устойчивое сопоставление областей даже при значительных геометрических искажениях.

В контексте задачи автоматической привязки изображений наиболее перспективным является объединение semantic-aware детекторов и локальных дескрипторов. Zero-Shot модели позволяют выделять устойчивые объекты интереса, а методы локального сопоставления обеспечивают точную оценку параметров преобразования между изображениями. Такой гибридный подход потенциально позволяет одновременно повысить точность привязки и уменьшить число итераций псевдоградиентной процедуры [10]. Особую важность может иметь аугментация данных с помощью дважды стохастических моделей [11, 12].

Для проведения исследования был сформирован синтетический набор данных, содержащий 6200 изображений разрешением 1024×1024 пикселей. Использование синтетических данных позволяет полностью контролировать параметры сцены и точно оценивать устойчивость алгоритмов к различным типам искажений. В качестве объектов интереса использовались здания, мосты, резервуары, промышленные сооружения, дорожная инфраструктура и транспортные средства [13]. Сцены генерировались в 3D-среде с различными условиями освещения и ракурсами наблюдения.

Для каждого исходного изображения автоматически создавался набор модифицированных вариантов. Использовались аффинные преобразования с изменением масштаба в диапазоне 0,7–1,3, поворот изображения на углы до $\pm 15^\circ$, сгор-преобразования с удалением до 40% области объекта, а также изменение яркости и контрастности. Дополнительно моделировались ошибки локализации путём искусственного смещения ограничивающей рамки на 10–30% относительно истинного положения объекта.

Пример синтетических сцен и используемых преобразований представлен на рисунке 1.

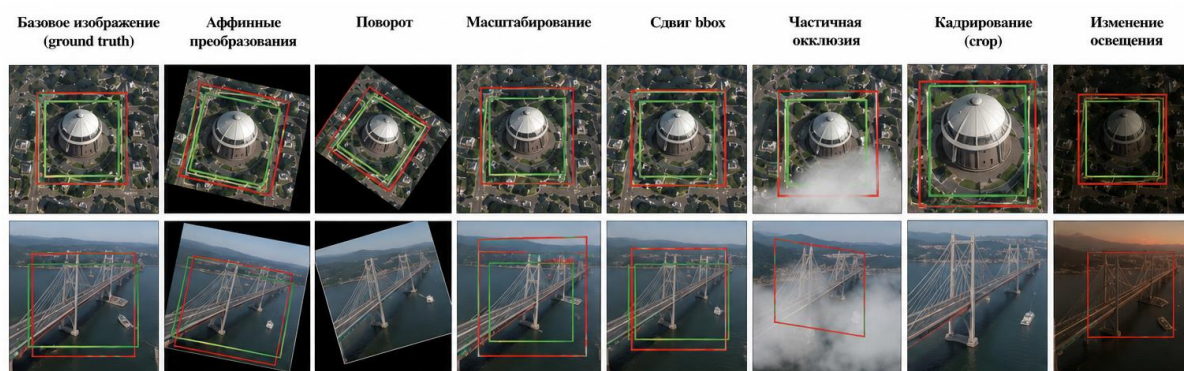


Рисунок 1. Синтетические сцены с вариациями геометрических и фотометрических преобразований, используемые для оценки устойчивости Zero-Shot моделей к сгор-искажениям, смещению bounding box и изменению масштаба

В состав датасета входили как простые сцены с одним объектом, так и сложные композиции с несколькими перекрывающимися объектами и неоднородным фоном. Это позволило исследовать устойчивость моделей к изменению структуры сцены и появлению ложных контуров. Отсутствие ограничивающих рамок на части объектов на рисунке 1 связано с особенностями работы Zero-Shot детекторов в условиях сильных геометрических и фотометрических искажений. При наличии сгор-преобразований, частичной окклюзии, размытия или значительного смещения объекта относительно центра сцены модель может не достигать порогового значения по уверенности, необходимой для формирования ограничивающего прямоугольника. Кроме того, в ряде случаев объект может быть распознан как фоновая структура вследствие недостаточной выраженности семантических признаков. Подобные ситуации были намеренно сохранены в примерах, поскольку они демонстрируют реальные ограничения Zero-Shot архитектур и позволяют визуально оценить различия в устойчивости моделей при работе с неполными или искажёнными данными.

В рамках исследования сравнивались четыре подхода:

- 1) случайный выбор отсчётов для псевдоградиентной процедуры;
- 2) использование YOLO-World в режиме Zero-Shot;
- 3) применение Grounding DINO с текстовыми подсказками;
- 4) ансамблевый метод, объединяющий результаты нескольких моделей.

Для модели YOLO выполнялось дополнительное трансферное обучение на 1800 размеченных изображениях синтетического набора. Это позволило сравнить supervised-подход с Zero-Shot архитектурами.

Предлагаемый ансамблевый метод включает несколько последовательных этапов. На первом этапе YOLO-World и Grounding DINO независимо формируют кандидаты в ограничивающие рамки. Далее выполняется объединение результатов и фильтрация пересекающихся областей при помощи Non-Maximum Suppression или других алгоритмов слияния детекторов [14]. После этого внутри найденных областей вычисляются локальные признаки SuperPoint. Финальное сопоставление выполняется алгоритмом SuperGlue с последующей геометрической верификацией методом RANSAC.

Общая схема ансамблевого поиска реперных областей и процедуры привязки изображений представлена на рисунке 2.

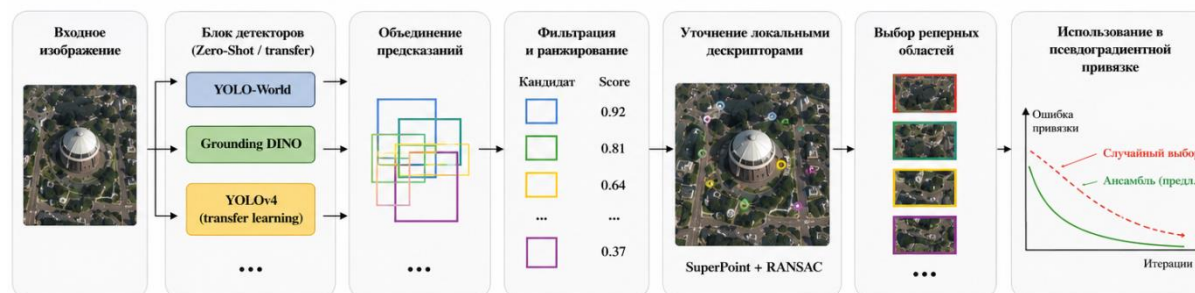


Рисунок 2. Архитектура ансамблевого метода поиска реперных областей на основе YOLO-World, Grounding DINO и локальных дескрипторов SuperPoint/SuperGlue для повышения точности привязки изображений

Для оценки эффективности использовались следующие метрики:

- mAP@0.5;
- Recall@0.5;
- средняя ошибка привязки;
- число итераций псевдоградиентной процедуры;
- вероятность успешной сходимости.

Результаты экспериментов показали, что использование semantic-aware реперных областей значительно повышает устойчивость псевдоградиентной процедуры привязки по сравнению со случайным выбором отсчётов. При случайном выборе точек наблюдалась высокая дисперсия ошибки, особенно при наличии окклюзии и сгор-преобразований. Модель YOLO-World продемонстрировала высокий баланс между скоростью и качеством локализации. Благодаря использованию open-vocabulary механизма модель успешно обнаруживала объекты даже при отсутствии специализированного обучения. Среднее значение mAP составило 0,58 при скорости обработки около 52 FPS. Grounding DINO обеспечила наиболее высокую точность локализации среди Zero-Shot моделей. Использование трансформерной архитектуры и мультимодального attention-механизма позволило повысить устойчивость к частичной окклюзии и сгор-преобразованиям. Наилучшие результаты были получены при использовании ансамблевого подхода. Комбинирование YOLO-World и Grounding DINO позволило объединить преимущества двух архитектур: высокую скорость первой модели и высокую точность второй. Результаты сравнения моделей показаны в таблице 1.

Таблица 1.

Сравнение моделей детектирования

Модель	mAP	FPS	Устойчивость
YOLO-World	0,58	52	0,81
Grounding DINO	0,61	18	0,87
YOLOv4 Transfer	0,74	65	0,79
Ансамбль	0,79	34	0,92

Анализ таблицы 1 показывает, что ансамблевый подход обеспечивает наиболее устойчивое выделение реперных областей. Несмотря на снижение скорости обработки по сравнению с YOLO-World, качество локализации и устойчивость к искажениям оказываются существенно выше. В таблице 2 представлены результаты экспериментов для привязки изображений.

Таблица 2.

Результаты привязки изображений

Метод	Ошибка, px	Итерации	Успешность
Случайный выбор	5,3	41	70%
YOLO-World	3,9	36	81%
Grounding DINO	3,6	34	84%
Ансамбль	2,2	29	94%

Из таблицы 2 видно, что использование semantic-aware реперных областей позволяет существенно снизить ошибку привязки изображений. При случайном выборе отсчётов средняя ошибка составляла 5,3 пикселя, тогда как ансамблевый подход уменьшил её до 2,2 пикселя.

В работе исследовано применение Zero-Shot моделей детектирования объектов для поиска реперных областей в задаче автоматической привязки изображений. Показано, что использование semantic-aware областей вместо случайного выбора отсчётов позволяет повысить устойчивость псевдоградиентной процедуры и снизить ошибку оценки параметров преобразования.

Сравнение YOLO-World, Grounding DINO и YOLOv4 с трансферным обучением показало, что Zero-Shot архитектуры обладают высокой обобщающей способностью и устойчивостью к искажениям сцены. YOLO-World обеспечивает оптимальный баланс скорости и качества, Grounding DINO демонстрирует наиболее точную локализацию объектов, а YOLO показывает высокую эффективность в рамках обученного домена.

Наилучшие результаты получены при использовании ансамблевого подхода, объединяющего YOLO-World, Grounding DINO и локальные дескрипторы SuperPoint/SuperGlue. Предложенный метод позволил более чем в два раза снизить ошибку привязки и повысить вероятность успешной сходимости до 94%.

Полученные результаты подтверждают перспективность интеграции Zero-Shot детекции объектов и самообучаемое сопоставление локальных признаков в задачах автоматической привязки изображений и системах технического зрения.

Благодарности

Работа выполнена при финансовой поддержке РНФ, Проект № 26-11-00336.

Литература

1. Lowe D. G. Distinctive Image Features from Scale-Invariant Keypoints // International Journal of Computer Vision. — 2004. — Vol. 60, No. 2. — P. 91–110. — DOI: 10.1023/B:VISI.0000029664.99615.94.
2. Bay H., Tuytelaars T., Van Gool L. SURF: Speeded Up Robust Features // Computer Vision – ECCV 2006 : 9th European Conference on Computer Vision, Graz, Austria, May 7–13, 2006 : Proceedings. — Berlin ; Heidelberg : Springer, 2006. — Vol. 3951. — P. 404–417. — DOI: 10.1007/11744023_32.
3. Redmon J., Divvala S., Girshick R., Farhadi A. You Only Look Once: Unified, Real-Time Object Detection // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). — Las Vegas, USA, 2016. — P. 779–788. — DOI: 10.1109/CVPR.2016.91
4. Bochkovskiy A., Wang C.-Y., Liao H.-Y. M. YOLOv4: Optimal Speed and Accuracy of Object Detection // arXiv preprint. — 2020. — arXiv:2004.10934. — URL: <https://arxiv.org/abs/2004.10934> (дата обращения: 12.05.2026).
5. Andriyanov N., Tashlinsky A., Dementiev V. Zero-Shot Detection in Satellite Images // 2025 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). — Tyumen, Russian Federation, 2025. — P. 1–5. — DOI: 10.1109/SYNCHROINFO65403.2025.11079342.
6. Cheng T., Song L., Ge Y., Liu W., Wang X., Shan Y. YOLO-World: Real-Time Open-Vocabulary Object Detection // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). — Seattle, USA, 2024. — P. 16901–16911.
7. Liu S., Zeng Z., Ren T., Li F., Zhang H., Yang J., Jiang Q., Li C., Yang J., Su H., Zhu J., Zhang L. Grounding DINO: Marrying DINO with Grounded Pre-training for Open-Set Object Detection // Computer Vision – ECCV 2024 : 18th European Conference, Milan, Italy, September 29 – October 4, 2024 : Proceedings. — Cham : Springer, 2024. — Vol. 15105. — P. 38–55.
8. DeTone D., Malisiewicz T., Rabinovich A. SuperPoint: Self-Supervised Interest Point Detection and Description // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPR Workshops). — Salt Lake City, USA, 2018. — P. 224–236.
9. Sarlin P.-E., DeTone D., Malisiewicz T., Rabinovich A. SuperGlue: Learning Feature Matching with Graph Neural Networks // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). — Seattle, USA, 2020. — P. 4938–4947.
10. Ташлинский А. Г., Кавеев И. Н., Воронов С. В. Методика привязки изображений в условиях интенсивных помех // Радиотехника. — 2012. — № 9. — С. 45–49.

11. Vasiliev K. K., Andriyanov N. A. Synthesis and Analysis of Doubly Stochastic Models of Images // CEUR Workshop Proceedings : Proceedings of the 2nd Workshop, Yekaterinburg, 15 November 2017. — Yekaterinburg, 2017. — P. 145–154.
12. Andriyanov N. A., Andriyanov D. A. The Using of Data Augmentation in Machine Learning in Image Processing Tasks in the Face of Data Scarcity // Journal of Physics: Conference Series : International Conference on Information Technology in Business and Industry (ITBI 2020), Novosibirsk, Russia, 6–8 April 2020. — Vol. 1661. — Bristol : IOP Publishing Ltd, 2020. — P. 012018. — DOI: 10.1088/1742-6596/1661/1/012018.
13. Andriyanov N. A., Dementiev V. E., Tashlinskiy A. G. Development of a Productive Transport Detection System Using Convolutional Neural Networks // Pattern Recognition and Image Analysis. Advances in Mathematical Theory and Applications. — 2022. — Vol. 32, No. 3. — P. 495–500. — DOI: 10.1134/S1054661822030038.
14. Kuttyrev A., Andriyanov N., Khort D., Smirnov I., Zubina V. Adaptive CNN Ensemble for Apple Detection: Enabling Sustainable Monitoring Orchard // AgriEngineering. — 2025. — Vol. 7, No. 11. — Art. 369. — DOI: 10.3390/agriengineering7110369.

RESEARCH OF ZERO-SHOT MODELS FOR REFERENCE REGION DETECTION AND IMAGE REGISTRATION ENHANCEMENT

N. Andriyanov

Financial University under the Government of the Russian Federation

The paper considers the problem of detecting reference regions in images for subsequent image registration. The influence of the stability of detected regions on the efficiency of the pseudo-gradient registration procedure is investigated using the Zero-Shot object detectors YOLO-World and Grounding DINO. An ensemble approach combining semantic-aware region detection and SuperPoint local descriptors is proposed. The study was conducted on a synthetic dataset consisting of 6200 images.



ОПТИЧЕСКИЕ НЕЙРОННЫЕ СЕТИ НА СТАТИЧЕСКИХ И ДИНАМИЧЕСКИХ ДАННЫХ: ИСТОРИЯ РАЗВИТИЯ И ТЕКУЩЕЕ СОСТОЯНИЕ

ст. преп., науч. сотр. Антонов Д.И.^{1,2}¹Ульяновский государственный технический университет²Ульяновский филиал Института радиотехники и электроники имени В. А. Котельникова РАН

В работе показаны этапы исторического развития оптических вычислений. Оптическая обработка информации начиналась с реализации преобразования Фурье на основе линз. Позднее был этап, в течение которого в оптоэлектронных устройствах создавались схемы на основе комбинирования логических операций. На сегодняшний день на переднем крае оптических вычислений находятся оптические нейронные сети, построенные как искусственный аналог биологических нейронных сетей. Биологические сети являются динамическими, поэтому среди искусственных нейронных сетей наиболее биоподобны именно динамические сети. Динамическими сетями, учитывающими временной фактор, являются оптические импульсные нейронные сети, один из вариантов которых рассмотрен в настоящей работе.

При разработке искусственной нейронной сети (ИНС) предполагается, что желаемый результат должен быть не хуже биологического аналога, а, возможно, и превосходить его. Одними из основных желаемых качеств ИНС (и устройств на основе ИНС) являются высокий уровень быстродействия и энергоэффективности. Потенциально этими качествами обладают устройства, в которых перенос информации осуществляется фотонами со скоростью света и с минимальными энергозатратами. Устройствами такого типа являются оптические нейронные сети (ОНС), являющиеся физической имплементацией ИНС с помощью оптических компонент.

Исторически оптическая обработка информации начиналась с использования преобразования Фурье, например, для целей пространственной фильтрации, с помощью линз. Создаваемые устройства основывались на свойствах световых волн, в частности, на том, что световые волны с различными длинами волн распространяются независимо друг от друга и могут быть разделены, что позволяет организовывать оптическую обработку информации.

Пример устройства для пространственной фильтрации на основе преобразования Фурье — система двойной дифракции — показан на рисунке 1. На вход устройства подаётся изображение, описываемое распределением $f(x, y)$, первая линза выполняет Фурье-преобразование изображения и далее в системе происходит свёртка с функцией рассеяния точки $h(x, y)$ (частный случай импульсной переходной функции, которая описывает выходной сигнал системы при подаче на вход сигнала в виде дельта-функции Дирака). Пространственный фильтр $H(\mu, \nu)$, являющийся преобразованием Фурье функции рассеяния точки, модулирует спектр, после чего происходит Фурье-преобразование модулированного сигнала второй линзой и выходное изображение $g(x, y)$ предстаёт как перевёрнутое входное изображение $f(x, y)$. Результатом работы системы является распределение амплитуды вида:

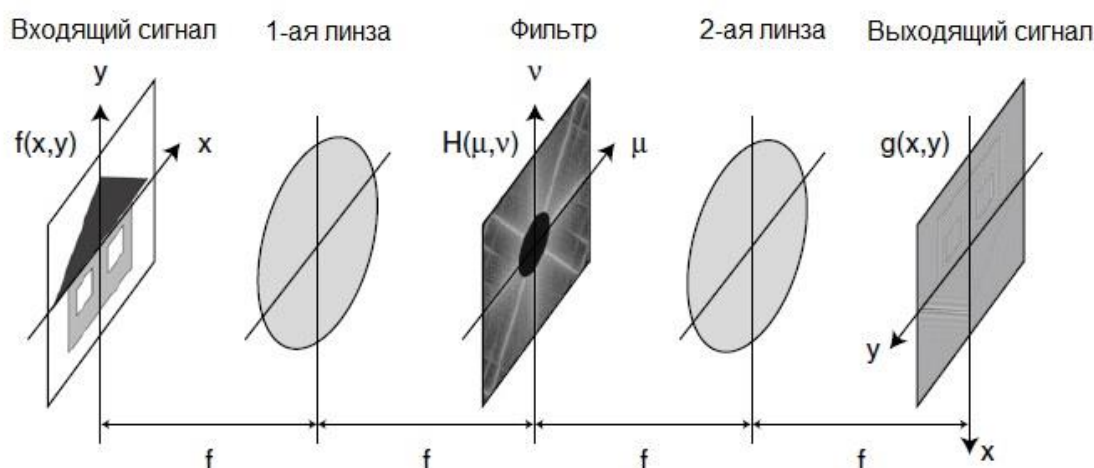


Рисунок 1. Пример оптического устройства для пространственной фильтрации, адаптировано из [1]

$$g(x, y) = \iint f(x', y') h(x - x', y - y') dx' dy' \quad (1)$$

В плоскости линзы выполняется Фурье-преобразование, в итоге чего уравнение (1) представимо в виде:

$$G(\mu, \nu) = F(\mu, \nu) H(\mu, \nu), \quad (2)$$

где $F(\mu, \nu)$ и $G(\mu, \nu)$ — спектры, соответственно, входного и выходного сигналов.

Отметим, что устройства для оптических вычислений на основе физических свойств света зачастую разрабатывались в виде гибридных оптико-электронных схем, которые имеют принципиально неустранимый недостаток, связанный с преобразованием энергии электронов в фотоны и обратно. Данный процесс потребляет около 30% энергии и замедляет передачу информации [1]; только полностью оптические устройства позволяют избежать потерь в скорости и энергии. Варианты пространственных модуляторов света используются в оптических системах для различных целей. Например, при использовании в качестве пространственных модуляторов жидкокристаллических ламп [2] или жидкокристаллических устройств на кремниевой подложке [3] можно динамически модулировать световые сигналы на двумерной плоскости.

В оптоэлектронных устройствах схемы реализуются путем комбинирования элементарных логических операций таких, как логическое И, логическое ИЛИ, исключающее ИЛИ. Логические операции нелинейны, что накладывает требования на характер оптических явлений в оптоэлектронных устройствах. Примером нестандартного подхода к разработке представления логических операций оптическими методами служит работа [4], в которой авторы реализовали нелинейные операции посредством процесса пространственного кодирования, что позволило использовать линейную оптическую систему для выполнения логических операций. В основе работы [4] лежит метод выполнения параллельных логических операций с использованием оптического теневого отражения, в рамках которого исходные пиксели изображения заменяются пространственным кодом, установленным в оптической проекционной системе.

Дальнейшее развитие оптических вычислений происходило во многом в связи с развитием ИНС, в которых элементы связаны между собой, что реализуемо с помощью технологии оптических межсоединений (interconnections). Первые работы в этом направлении содержали большое количество оригинальных подходов.

В ранних работах по ОНС, в частности, применялась анаморфная оптика, которая исходно предназначалась для изменения изображений посредством их масштабирования в различных пропорциях по двум взаимно перпендикулярным направлениям таким образом, что в результате из квадрата получался прямоугольник или ромб, из круга — эллипс. Анаморфная оптика использовалась в ОНС для выполнения векторно-матричного умножения [5, 6], что позволяло с её помощью строить полносвязную нейронную сеть Хопфилда с симметричной матрицей связей, в классическом случае имеющую один слой нейронов.

Интересным вариантом реализации ОНС было построение сети на основе использования объемных голографических межсоединений в фоторефрактивных кристаллах [7]. Объемные голограммы (рисунок 2) позволяют хранить большое количество межсоединений на единицу объема, а использование фоторефрактивных кристаллов позволяет динамически изменять свойства этих соединений, что позволяет обучать сеть. Линзы на рисунке 2 преобразуют пространственное положение каждого нейрона в пространственную частоту света, излучаемого нейроном или падающим на него. Связь между нейроном во входном слое и нейроном в выходном слое формируется путем интерференции света, излучаемого входным нейроном, со светом, излучаемым нейроном обучающего слоя. Интерференция обучающего сигнала и входного сигнала создает в записывающей среде (в голограмме) решетку.

Дальнейшее развитие ОНС позволило выделить ряд подходов в реализации сетей, отметим некоторые из них.

Отдельно стоит подход, который позволил создать вид ОНС, выделяющийся из общего множества оптических сетей, — метод резервуарных вычислений. Резервуарная ОНС содержит резервуарный слой; входные сигналы поступают в резервуар, осуществляющий нелинейные преобразования, которые зависят от предыстории. В резервуарных ОНС обучаются только веса связи от резервуара к выходному слою. Помимо общих принципов, реализация резервуарных ОНС предполагает разнообразные варианты, например, разработаны варианты с оптическими волоконными кольцами [8], на лазерах с оптической обратной связью и инъекцией [9] и т.д.

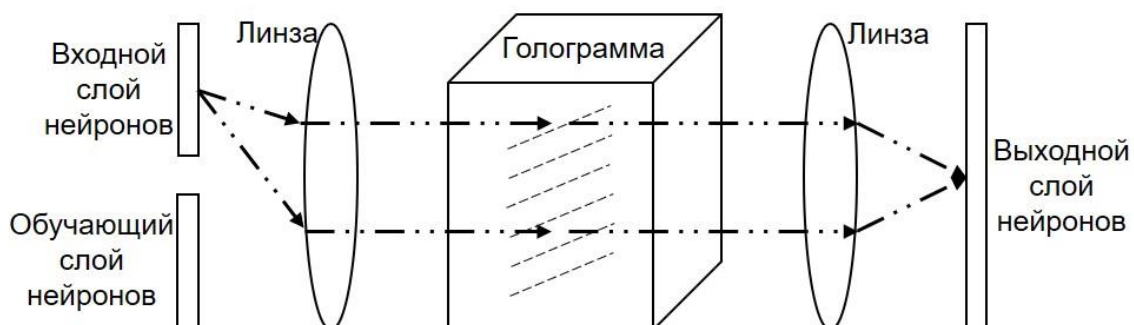


Рисунок 2. Принципиальная архитектура ОНС с объемной голограммой, адаптировано из [7]

Обучение зачастую определяет архитектуру и принципы работы ОНС. Упростить поиск приемлемой архитектуры пытаются, в частности, тем, что выполняют обучение ОНС с помощью компьютера (*in silico*), обучая «цифрового двойника» ОНС методом обратного распространения ошибки. После завершения обучения «цифрового двойника» рассчитанные значения весов переносятся на оптические элементы ОНС. Такой подход требует сравнительно много времени для обучения и проигрывает неоптическим ИНС в точности [10]. Был разработан способ обучения ОНС, также использующий обучение *in silico*, но с лучшей точностью — гибридное обучение на компьютере «с учётом физики» [11]. В рамках этого варианта ОНС при обучении методом обратного распространения ошибки прямой проход с вычислением функции потерь выполняется на оптическом оборудовании, а обратный проход — на компьютере. Ввиду того, что часть операций происходит на оптическом оборудовании, сокращается диспропорция данных между «физической» частью ОНС и «цифровым двойником».

Из нейробиологии известны свойства биологических нейронных сетей, позволяющие им эффективно функционировать, аналоги которых используются в ИНС. Укажем некоторые из этих свойств, использованных в описанной ниже модели, которые позволяют создать наиболее биоподобные нейроморфные ОНС:

- 1) важным является умение биологических сетей оперировать с динамическими данными; учёт фактора времени позволяет ОНС также работать с динамическими данными;
- 2) биологические сети кодируют информацию с помощью импульсов (спайков), ОНС также могут быть реализованы в виде импульсной нейронной сети (ИМНС) на оптическом оборудовании, оптические ИМНС являются динамическими сетями;
- 3) синаптическая пластичность используется при обучении сети и позволяет осуществлять эффективную синаптическую передачу сигнала; для реализации синаптической пластичности в ОНС используются специальные материалы, например, способные изменять коэффициент отражения или пропускания света в зависимости от интенсивности входящего света.

Примером, объединяющим в себе эти свойства, служит ОНС, описанная в работе [12], на основе которой удобно рассмотреть особенности функционирования динамических ОНС.

Специальным материалом, использованном в работе ОНС [12], является $Ge_2Sb_2Te_5$ (германий-сурьма-теллур или GST) — материал с фазовым переходом из группы халькогенидных стёкол, который, в частности, который используется в перезаписываемых оптических дисках и в фотонных интегральных схемах (photonic integrated circuit, PIC), где им осуществляется сдвиг фазы света на π . Данный материал с изменением фазы (phase-change material, PCM) изменяет фазовое состояние под воздействием низкоинтенсивного лазерного излучения: фазовый переход в кристаллическое состояние происходит при нагреве GST до температуры кристаллизации $100 \div 150$ °C (температура плавления 600 °C). Аморфная фаза GST имеет более низкую отражательную способность, чем кристаллическая.

Существенными для использования в ОНС являются следующие свойства GST:

- время рекристаллизации - 20 нс, что обеспечивает высокую скорость переключения,
- материал выдерживает более 10^{13} циклов изменения фазы без потери свойств и длительное хранение данных (более 10 лет),
- предел масштабирования ограничен возможностями литографии - не менее 45 нм.

ОНС в [12] является полностью оптической ИМНС с возможностью обучения, т.е. для её функционирования не требуется вспомогательных компьютеров, выполняется непосредственное обучение ОНС. Достигается это за счёт механизма работы нейрона, где основными частями являются синаптические связи на основе GST, кольцевые резонаторы и мультиплексор.

Базовый элемент («оптический нейрон») ОНС (рисунок 3) содержит синапсы, реализованные в виде РСМ-ячеек на основе GST, расположенных поверх оптических волноводов (площадь РСМ-ячейки $3,6 \text{ мкм}^2$). Синаптический волновод с РСМ-ячейкой в аморфном состоянии является высокопропускаемым для света, осуществляя сильную связь между двумя нейронами. Когда РСМ-ячейка находится в кристаллическом состоянии, большая часть света поглощается, что приводит к слабому соединению. Нейрон содержит 4 малых кольцевых резонатора различных радиусов, которые используются для подачи волн разной длины от входных сигналов в один волновод для мультиплексирования, ведущий к большому резонатору с РСМ-ячейкой. Сигналы, подходящие к нейрону, проходят через синапс и поступают на малые кольцевые резонаторы, формирующий сигналы с разной длиной волны. Все сигналы поступают в один волновод — мультиплексор, обеспечивающий возможность параллельного прохождения сигналов с разными длинами волн без смешивания. Мультиплексор выводит сигнал на кольцевой резонатор, работающий в качестве сумматора.

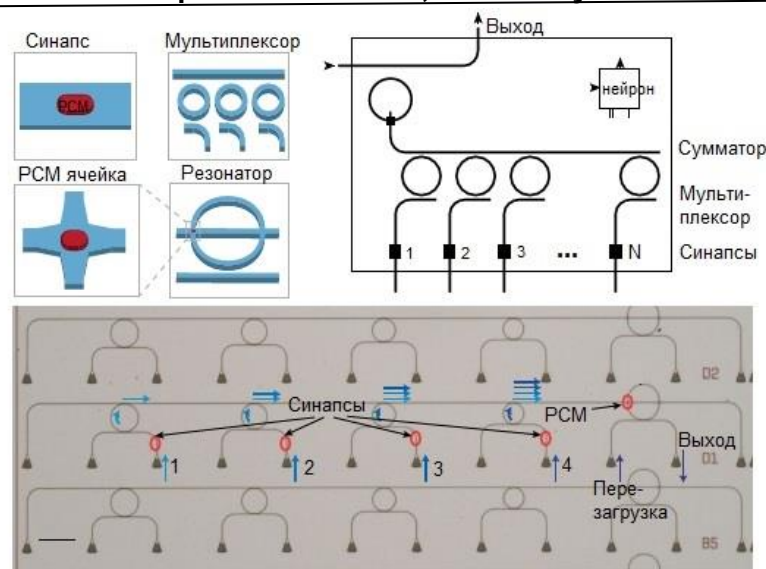


Рисунок 3. Полностью оптическая ОНС, адаптировано из [12]

В ситуации, когда РСМ-ячейка кольцевого резонатора находится в кристаллическом состоянии, зондирующий импульс, отправленный по «выходному» волноводу, попадает в кольцевой резонатор, откуда никуда не поступает далее, и в итоге выходной импульс не будет наблюдаться. Но если суммарная мощность взвешенных входных импульсов от пресинаптических нейронов достаточно высока, чтобы переключить РСМ-ячейку в аморфное состояние, то зондирующий импульс будет передаваться мимо кольца, генерируя выходной импульс. При достижении суммарной мощностью импульсов пороговой мощности происходит переключение РСМ-ячейки на кольцевом резонаторе и генерируется выходной импульс.

История развития оптических вычислений, которая начиналась как преобразования Фурье на линзах, сегодня дошла до создания динамических ОНС. Ожидается, что оптические вычислительные технологии, являющиеся наиболее высокоскоростными и энергоэффективными, будут становиться все более важными в будущем. Предположительно, уже в ближайшее время они будут применяться в периферийных устройствах Интернета вещей, использующих характеристики оптических технологий. Сочетание информационных технологий с современными оптическими технологиями открывает новые горизонты в информатике.

Работа выполнена при поддержке Минобрнауки РФ в рамках Государственного задания ИРЭ им. В.А. Котельникова РАН (FFWZ-2025-0005).

Литература

1. Photonic Neural Networks with Spatiotemporal Dynamics. Paradigms of Computing and Implementation / edited by H. Suzuki, J. Tanida, M. Hashimoto. – Springer. – 2024. – URL: <https://link.springer.com/book/10.1007/978-981-99-5072-0>.
2. Bleha W.P. Application of the liquid crystal light valve to real-time optical data processing / W.P. Bleha, L.T. Lipton, E. Wiener-Avnear, J. Grinberg, P.G. Reif, D. Casasent, H.B. Brown, B.V. Markevitch // Optical Engineering. – Vol. 17 (4). - 1978. – p. 174371. <https://doi.org/10.1117/12.7972245/>.
3. Lazarev G. LCOS Spatial Light Modulators: Trends and Applications / G. Lazarev, A. Hermerschmidt, S. Krüger, S. Osten // in Optical Imaging and Metrology: Advanced Technologies. - Wiley-VCH Verlag GmbH & Co. KGaA. - 2012. - pp.1–29.
4. Tanida J. Optical logic array processor using shadowgrams / J. Tanida, Y. Ichioka // J. Opt. Soc. Am. – Vol. 73(6). - 1983. – p. 800–809. - <https://doi.org/10.1364/JOSA.73.000800>.
5. Goodman J.W. Fully parallel, high-speed incoherent optical method for performing discrete fourier transforms / J.W. Goodman, A.R. Dias, L.M. Woody // Optic Letters. – Vol. 2(1). – 1978. - p. 1–3. - <https://doi.org/10.1364/OL.2.000001>.
6. Psaltis D. Optical information processing based on an associative-memory model of neural nets with thresholding and feedback / D. Psaltis, N. Farhat // Optic Letters. – Vol. 10(2). – 1985. -p. 98–100. - <https://doi.org/10.1364/OL.10.000098>.

7. Psaltis D. Adaptive optical networks using photorefractive crystals / D. Psaltis, D. Brady, K. Wagner // *Applied Optics*. – Vol. 27 (9). - 1988. – p. 1752–1759. -<https://doi.org/10.1364/AO.27.001752>.
8. Duport F. All-optical reservoir computing / F. Duport, B. Schneider, A. Smerieri, M. Haelterman, S. Massar // *Optics Express*. – Vol. 20 (20). – 2012. – p. 22783–22795. -<https://doi.org/10.1364/OE.20.022783>.
9. Nakayama J. Laser dynamical reservoir computing with consistency: an approach of a chaos mask signal / J. Nakayama, K. Kanno, A. Uchida // *Optics Express*. – Vol. 24(8). – 2016. – p. 8679–8692. -
<https://doi.org/10.1364/OE.24.008679>.
10. Patterson D. Carbon emissions and large neural network training / D. Patterson, J. Gonzalez, Q. Le et al. // *arXiv preprint*. – 2021. - arXiv:2104.10350.
11. Wright L.G. Deep physical neural networks trained with backpropagation / L.G. Wright, T. Onodera, M.M. Stein et al. // *Nature*. – 2022. - Vol. 601. - No. 7894. - p. 549–555.
12. Feldmann J. All-optical spiking neurosynaptic networks with self-learning capabilities / J. Feldmann, N. Youngblood, C.D. Wright et al. // *Nature*. – Vol. 569. – 2019. – p. 208–214. <https://doi.org/10.1038/s41586-019-1157-8>.

OPTICAL NEURAL NETWORKS USING STATIC AND DYNAMIC DATA: HISTORY OF DEVELOPMENT AND CURRENT STATUS

Senior Lecturer, Researcher D.I. Antonov

Ulyanovsk State Technical University

Ulyanovsk Branch of Kotelnikov Institute of Radioengineering and Electronics of Russian Academy of Sciences

This article describes the stages in the historical development of optical computing. Optical information processing began with the introduction of the lens-based Fourier transform. Later, circuits based on combinations of logical operations appeared in optoelectronic devices. Today, optical neural networks, built as artificial analogs of biological neural networks, are at the forefront of optical computing. Biological networks are dynamic, so among artificial neural networks, dynamic networks are the most bioinspired. Time-aware dynamic networks include optical spiking neural networks, a variant of which is discussed in this paper.



ПРЕДОБРАБОТКА В РЕАЛЬНОМ ВРЕМЕНИ СЕРИИ СНИМКОВ С БПЛА ДЛЯ ИХ СОВМЕЩЕНИЯ СО СПУТНИКОВЫМИ ИЗОБРАЖЕНИЯМИ

проф. Ташлинский А.Г., студ. Белов А.А.

Ульяновский государственный технический университет,

Предложена методика совмещения в реальном времени нескольких изображений, последовательно получаемых с камеры БПЛА, с одновременной компенсацией их взаимных проективных искажений и переводом в систему географических координат EPSG:3395. Методика направлена на последующую привязку пространственно совмещенных аэроизображений к спутниковым изображениям для их совместной обработки. В основе совмещения изображений с камеры БПЛА лежит рекуррентная псевдоградиентная процедура, что позволило получить высокое быстродействие и работоспособность в условиях априорной неопределенности. Перевод совмещенных изображений производится в систему географических координат EPSG:3395. Разработано программное обеспечение на языке C++ с использованием библиотеки OpenCV с открытым исходным кодом, подтвердившее эффективность методики на реальных последовательностях снимков с камер БПЛА. Программная реализация перенесена на одноплатные компьютеры Raspberry и Radxa, работа которых опробована в реальном времени на борту БПЛА.

Постановка задачи

Применение беспилотных летательных аппаратов (БПЛА) в различных сферах человеческой деятельности постоянно растет. Неотъемлемой составляющей БПЛА являются камеры, формирующие изображения и видео различного назначения. Обработка изображений и видео с камер БПЛА для решения различных практических задач стала самостоятельным научным направлением. Одной из таких задач является совмещение спутниковых и аэроизображений БПЛА для их дальнейшей совместной обработки [1, 2]. Решение этой задачи затрудняют проективные искажения [3] изображений с камер БПЛА, которые возникают, когда главная оптическая ось камеры БПЛА отклонена от ее ортотрансформированного положения по отношению к земной поверхности, то есть при ненулевых углах Эйлера [4].

При наличии у камеры БПЛА гиropодвеса для компенсации искажений можно использовать привязку смежных кадров [5]. Но при этом мы получаем только оценку параметров расхождения взаимных проективных искажений кадров. При отсутствии гиросtabilизации оптической системы БПЛА для компенсации проективных искажений можно использовать значения углов Эйлера [6] с инерциальной системы (углов тангажа, крена и рысканья), синхронизированные с видеопоследовательностью. Одному из вариантов такого подхода посвящено настоящее исследование.

В рамках исследования поверхность Земли считалась плоской. Такое допущение для снимков с камер БПЛА самолетного типа с фокусным расстоянием порядка 50 мм является приемлемым и общепринятым уже при высоте полета более 400 м. На практике же высота полета БПЛА этого класса, как правило, значительно выше.

Механизм возникновения проективных искажений подробно рассмотрен в работе [7]. Там же показано, что в трехмерном пространстве точке с координатами (X, Y, Z) на ненормализованном изображении, на нормализованном изображении будут соответствовать координаты:

$$\begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = \mathbf{M} \cdot \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}, \quad (1)$$

где $\mathbf{M} = \mathbf{M}(\alpha)\mathbf{M}(\omega)\mathbf{M}(\kappa) =$

$$\begin{pmatrix} \cos\omega \cdot \cos\kappa & -\cos\omega \cdot \sin\kappa & \sin\omega \\ \cos\alpha \cdot \sin\kappa + \sin\omega \cdot \sin\alpha \cdot \cos\kappa & \cos\alpha \cdot \cos\kappa - \sin\omega \cdot \sin\alpha \cdot \sin\kappa & -\cos\omega \cdot \sin\alpha \\ \sin\alpha \cdot \sin\kappa - \cos\alpha \cdot \sin\omega \cdot \cos\kappa & \sin\alpha \cdot \cos\kappa + \cos\alpha \cdot \sin\omega \cdot \sin\kappa & \cos\omega \cdot \cos\alpha \end{pmatrix};$$

$\mathbf{M}(\alpha)$, $\mathbf{M}(\omega)$ и $\mathbf{M}(\kappa)$ – матрицы поворота, задаваемые углами тангажа α , крена ω и рысканья κ соответственно.

При этом с учетом известного фокусного расстояния F камеры связь координат (x', y') точки нормализованном изображении в локальной системе координат кадра с трехмерными координатами определяется выражением:

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} -\frac{Z' \cdot x'}{F} \\ -\frac{Z' \cdot y'}{F} \end{pmatrix}. \quad (2)$$

Для примера на рисунке 1а приведено реальное изображение с камеры БПЛА, полученное при углах тангажа, крена и рысканья 0,1097, 0,2349 и 0,029123 радиан соответственно, а на рисунке 1б – то же изображение с коррекцией проективных искажений (далее такие изображения называются нормализованными).

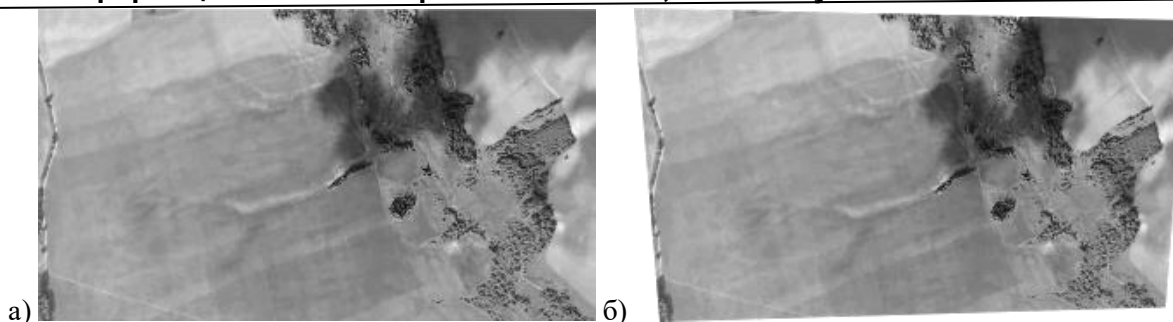


Рисунок 1. Пример изображения с камеры БПЛА (а) и его нормализованный вид (б)

Задачей исследования является разработка методики получения по известным углам крена, тангажа и рыскания БПЛА из текущего кадра изображения нормализованного изображения, совмещение (сшивки) нескольких последовательно получаемых нормализованных изображений в единое и перевод его из локальной системы координат кадра в глобальные географические координаты, в формат, который непосредственно может быть использован для совмещения со спутниковыми изображениями.

Совмещение нормализованных изображений

Сшивка нормализованных изображений рассмотрена на примере совмещения условно опорного $\mathbf{Z}'_r$ и совмещаемого $\mathbf{Z}'_c$ изображений. При этом расширение на большее число совмещаемых изображений является очевидным. Для нахождения вектора параметров $\vec{\alpha}$ совмещения применена псевдоградиентная адаптация [8], предполагающая задание модели взаимных пространственных деформаций $\mathbf{Z}'_r$ и $\mathbf{Z}'_c$ с параметрами $\vec{\alpha}$, а также целевой функции J качества совмещения. Удобной процедурой нахождения экстремума функции J в пространстве параметров $\vec{\alpha}$ является [9]:

$$\hat{\vec{\alpha}}_t = \hat{\vec{\alpha}}_{t-1} - \Lambda_t \cdot \nabla J(\hat{\vec{\alpha}}_{t-1}, \tilde{\mathbf{Z}}'_{rt}, \mathbf{Z}'_c), \quad (3)$$

где: $\hat{\vec{\alpha}}_t$ – вектор оценок параметров совмещения, сформированный на t -й итерации; Λ_t – матрица обучения, задающая шаг изменения оценок; $\nabla J(\cdot)$ – псевдоградиент функции качества $J(\hat{\vec{\alpha}}_{t-1}, \tilde{\mathbf{Z}}'_{rt}, \mathbf{Z}'_c)$; $\tilde{\mathbf{Z}}'_{rt}$ – передискретизированное по текущим оценкам $\hat{\vec{\alpha}}_{t-1}$ опорное изображение $\mathbf{Z}'_r$; $t = \overline{1, T}$ – номер итерации. С учетом анализа, проведенного в [10] был применен частный случай (3) – релейная псевдоградиентная процедура:

$$\hat{\vec{\alpha}}_t = \hat{\vec{\alpha}}_{t-1} - \Lambda \cdot \text{sign} \nabla J(\hat{\vec{\alpha}}_{t-1}, \mathbf{Z}'_t), \quad (4)$$

где: $\mathbf{Z}'_t$ – локальная выборка из μ пикселей $\tilde{z}'_{(x,y)_j} \in \tilde{\mathbf{Z}}'_{rt}$ и $z'^c_{(x,y)_j} \in \mathbf{Z}'_c$, $(x, y)_j$ – координаты j -го пикселя, $j = \overline{1, \mu}$.

Процедура (4) обеспечивает устойчивую сходимость оценок параметров совмещения и работоспособность в условиях априорной неопределенности.

При реализации (4) пиксели $z'^c_{(x,y)_j}$ на совмещаемом изображении $\mathbf{Z}'_c$ выбирались случайным образом, а $\tilde{z}'_{(x,y)_j}$ брались из передискретизированного $\tilde{\mathbf{Z}}'_{rt}$ с теми же координатами. Яркость $\tilde{z}'_{(x,y)_j}$ при передискретизации находилась с использованием билинейной интерполяции.

Поскольку в решаемой задаче изображения формируются в схожих условиях освещенности в качестве целевой функции был выбран средний квадрат разности яркостей изображений [5], как требующий небольших вычислительных затрат. Анализ также показал, что в качестве модели взаимных деформаций для нормализованных изображений достаточно модели подобия [11], имеющей вектор параметров $\vec{\alpha} = (k, \varphi, l_x, l_y)$, где k – коэффициент масштаба, φ – угол поворота, l_x, l_y – сдвиг.

Перевод локальной системы координат кадра в географическую систему координат

Найдено соответствие между координатами точки нормализованного изображения в локальной системе координат кадра и географическими координатами на земной поверхности. При этом использована система координат EPSG:3395, представляющая собой проекцию Меркатора [12] на эллипсоид WGS-84, применяемая, например, в Яндекс-картах.

Область земной поверхности в системе EPSG:3395, соответствующую кадру изображения с камеры БПЛА, условно назовем «картой». Будем считать, что в момент формирования кадра известны угол рыскания κ_0 , высота H_0 БПЛА, а также его географические координаты (λ_0, ψ_0) , где λ – долгота, ψ – широта (например, по GPS). При этом этим координатам в локальной системе координат кадра соответствует точка $(0, 0)$.

Учитывая (6), для точки S в локальной системе координат карты метрические координаты (в метрах) можно найти как:

$$\begin{pmatrix} X'_S \\ Y'_S \end{pmatrix} = \begin{pmatrix} k_H(x'_S \cdot \cos(\kappa_0) - y'_S \cdot \sin(\kappa_0)) \\ k_H(x'_S \cdot \sin(\kappa_0) + y'_S \cdot \cos(\kappa_0)) \end{pmatrix}, \quad (5)$$

где: $k_H = H_0 \cdot l_{px} \cdot q / F$; l_{px} – физический размер пиксела матрицы (в метрах); q – множитель, определяемый отношением максимального разрешения камеры (в пикселах) к используемому разрешению [13].

При задании карты в виде прямоугольника со сторонами параллельными меридианам и параллелям нужно определить минимальную и максимальную координаты по горизонтальной и вертикальной осям карты, которые и определяют размеры прямоугольника.

Заметим, что для нахождения координат в глобальной метрической системе (в метрах) нужно выражения (5) умножить на поправочный коэффициент k_ψ [14], определяемый формулой:

$$k_\psi = \frac{\cos(\psi)}{\sqrt{1 - c^2 \cdot \sin^2(\psi)}}, \quad (6)$$

где: ψ – широта точки, для которой рассчитываются координаты в метрах, c – эксцентриситет эллипсоида WGS-84.

Метрические координаты (X, Y) , соответствующие географическим координатам (λ, ψ) , на карте по долготе определяется соотношением:

$$Y = a \cdot k_\psi \cdot \ln \left(\operatorname{tg} \left(\frac{\pi}{4} + \frac{\psi}{2} \right) \cdot \chi^{\frac{c}{2}}(\psi) \right), \quad (7)$$

а по широте:

$$X = a \cdot k_\psi \cdot \lambda, \quad (8)$$

где: $\chi(\psi) = (1 - c \cdot \sin(\psi)) / (1 + c \cdot \sin(\psi))$; $a = 6378136$ метров – большая полуось эллипсоида WGS-84; $c = 0,081819191$ [15].

Для перехода от метрических координат карты к ее географическим координатам определим вначале на карте метрические координаты точки, соответствующей началу координат в локальной системе кадра:

$$\begin{pmatrix} X_0 \\ Y_0 \end{pmatrix} = \begin{pmatrix} a \cdot k_\psi \cdot \lambda_0 \\ a \cdot k_\psi \cdot \ln \left(\operatorname{tg} \left(\frac{\pi}{4} + \frac{\psi_0}{2} \right) \cdot \chi^{\frac{c}{2}}(\psi_0) \right) \end{pmatrix}. \quad (9)$$

Поскольку в проекции Меркатора на эллипс долгота линейно зависит от расстояния от начала координат [16], то при размере кадра $M \times N$ долготу произвольной точки (x', y') нормализованного изображения можно найти как:

$$\lambda^* = \frac{X_0 + \frac{x'}{M} (X'_{\max Y} - X'_{\min Y}) \cdot \cos(\kappa_0) + \frac{y'}{N} (Y'_{\max X} - Y'_{\min X}) \cdot \sin(\kappa_0)}{a \cdot k_\psi}, \quad (10)$$

где $(X'_{\min Y}, X'_{\max Y})$ и $(Y'_{\min X}, Y'_{\max X})$ – минимальные и максимальные метрические координаты области карты по базовым осям, соответствующие угловым точкам одной стороны кадра и рассчитанные в соответствии с (5).

Для широты аналогичная линейность не соблюдается, поэтому для ее определения используем известный итерационный алгоритм [17], который позволяет с небольшими вычислительными затратами найти нелинейное изменение географической координаты относительно ее положения в регулярной метрической сетке отсчетов.

Соответствие географических координат локальным координатам (x'_r, y'_r) точек нормализованного совмещаемого изображения(й) Z'_c ищется аналогично, с той разницей, что координаты (x'_r, y'_r) определяются через оценки параметров деформаций совмещаемого кадра относительно опорного. В частности, при использовании для оценивания деформаций модели подобия:

$$\begin{pmatrix} x'_r \\ y'_r \end{pmatrix} = \begin{pmatrix} \hat{k}(x'_d \cdot \cos(\hat{\varphi} + \kappa) - y'_d \cdot \sin(\hat{\varphi} + \kappa)) + \hat{l}_x \\ \hat{k}(x'_d \cdot \sin(\hat{\varphi} + \kappa) + y'_d \cdot \cos(\hat{\varphi} + \kappa)) + \hat{l}_y \end{pmatrix}, \quad (11)$$

где: (x'_d, y'_d) – координаты точек нормализованного деформированного кадра; $\hat{k}$, $\hat{\varphi}$, $\hat{l}_x$ и $\hat{l}_y$ – оценки параметров модели подобия, полученные в результате псевдоградиентного оценивания. При этом если высота БПЛА в момент получения совмещаемого кадра изменилась, то это нужно учесть в формуле (5).

Экспериментальные результаты

Для проверки корректности полученных расчетных выражений на реальных последовательностях снимков с камер БПЛА было разработано программное обеспечение на языке C++ с использованием библиотеки OpenCV с открытым исходным кодом. Программная реализация перенесена на одноплатные компьютеры Raspberry Pi 4B 8GB и Radxa Rock 5 model A 16GB, работа которых опробована в реальном времени на борту БПЛА.

В эксперименте использована камера с фокусным расстоянием 50 мм, разрешением 1920x1080 и частота кадров 30 Гц. Данные по углам Эйлера и высоте БПЛА поступали синхронно с кадрами видео, информация с GPS – асинхронно. Высота полета для результатов, приведенных ниже, составляла около 900 м. Угол крена в рамках одной пары кадров на участках поворота БПЛА менялся в пределах до 17 градусов, другие углы Эйлера изменялись меньше.

При совмещении изображений в центральной части их совместной области достигалась субпиксельная точность, на границах погрешность совмещения достигала до 6 пикселей, в среднем примерно 1,5-2. Увеличение погрешности на периферии связано с недокомпенсацией проективных искажений, в частности, из-за погрешностей углов Эйлера, рельефа местности и оптических искажений, вызванных конечностью апертуры.

Полученные результаты подтвердили адекватность аналитических зависимостей. Скорость обработки на Raspberry составила 10 кадров в секунду (через 2 кадра), на Radxa – до 16 кадров в секунду.

Пример исходного кадра изображения и его нормализованного вида с компенсированными проективными искажениями приведен на рисунке 1. Пример другого кадра изображения из той же видеопоследовательности, полученного при $\alpha = 0,13621$, $\omega = 0,26985$ и $\kappa = -0,44428$ радиан, приведен на рисунке 2. Там же показан его нормализованный вид. Пример совмещения ненормализованных изображений, приведенных на рисунках 1 и 2, с применением процедуры (4) показан на рисунке 3а. Для удобства визуального анализа совмещаемые изображения показаны чередующимися полосами и у одного из них изменен контраст. Видно, что в центральной части изображения совмещены, однако на краях качество совмещения явно неудовлетворительное, что объясняется значительными взаимными проективными искажениями. Совмещение нормализованных изображений рисунков 1 и 2 приведено на рисунке 3б, на котором уже отмечается высокое качество совмещения на всей области пересечения изображений.

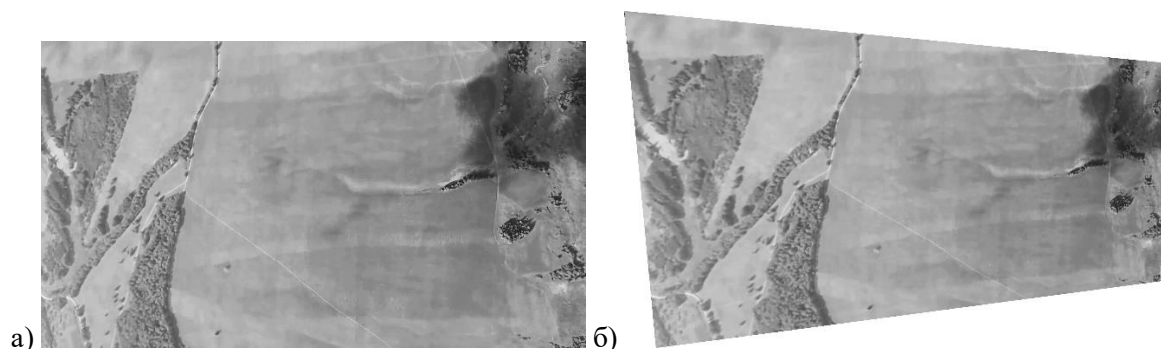


Рисунок 2. Пример изображения с камеры БПЛА (а) и его нормализованный вид (б)

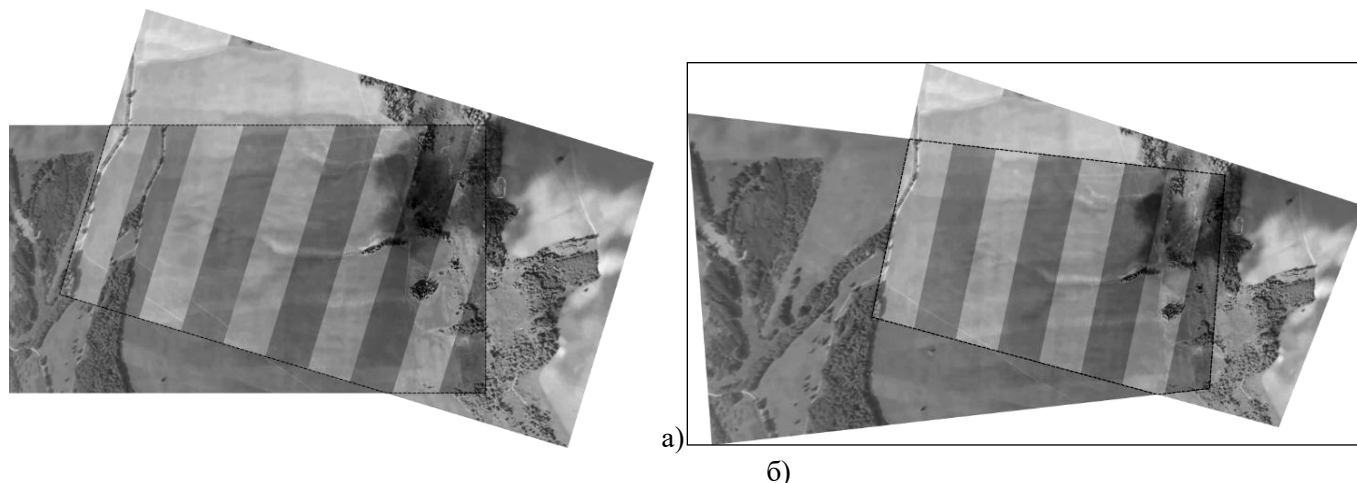


Рисунок 3. Совмещение изображений без (а) и с компенсаций (б) проективных искажений

Фрагмент Яндекс-карты, полученный переводом совмещенных изображений (рисунок 4а) в географические координаты, приведен на рисунке 4б. Видно хорошее соответствие нормализованных изображений с камеры БПЛА и сформированного изображения Яндекс-карты. Учитывая малое расхождение в геометрии этих изображений, обеспечить их совмещение не является сложной задачей, в частности, с использованием псевдоградиентных процедур [5].

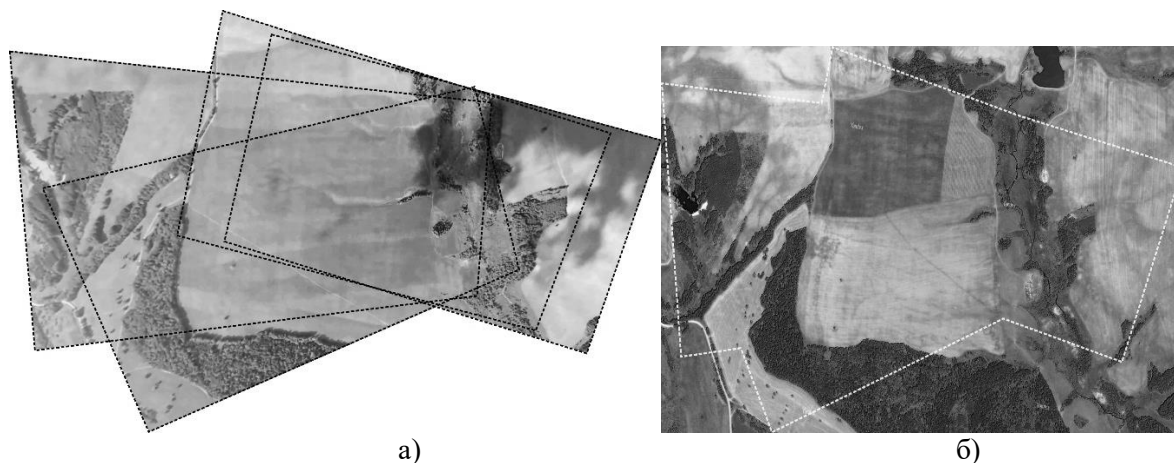


Рисунок 4. Пример сшивки 4 кадров с компенсацией проективных искажений и фрагмент Яндекс-карты, соответствующий сшивке

Заключение

Разработанная методика совмещения изображений, формируемых камерой БПЛА, с предварительной коррекцией их проективных искажений и переводом совмещенных изображений в географические координаты, ориентированная на последующее совмещение результата со спутниковыми изображениями, показала высокую эффективность. Она ориентирована на использование в условиях ограниченных вычислительных ресурсов и реализацию на недорогих и компактных вычислительных платформах.

Исследование выполнено за счет гранта РНФ № 26-11-10336,

<https://rscf.ru/project/26-11-10336>.

Литература

- Zhuang J., Dai M., Chen X., Zheng E. A faster and more effective cross-view matching method of UAV and satellite images for UAV geolocalization. *Remote Sensing* 2021; 13(19), 3979.
- Wang H., Shen Q., Deng Z., Cao X., Wang X. Absolute pose estimation of UAV based on large-scale satellite image. *Chinese Journal of Aeronautics* 2024; 37(6): 219-231.
- Hartley R., Zisserman A. *Multiple View Geometry in Computer Vision*. Cambridge: Cambridge University Press; 2003.
- Агапов С.В. *Фотограмметрия сканерных снимков*. М.: Картгеоцентр – Геоиздат; 1996.
- Tashlinskii A.G. Optimization of Goal Function Pseudogradient in the Problem of Interframe Geometrical Deformations Estimation. *Pattern Recognition Techniques, Technology and Applications*. London, United Kingdom: IntechOpen; 2008.
- Платонов А.К. Определение параметров проективного отображения в зрительном канале робота. *Препринты ИПМ им. М.В. Келдыша*; 2007; 39.
- Ташлинский А.Г., Белов А.А., Сафина Г.Л. Преобразование серии снимков камеры БПЛА для совместной обработки со спутниковыми изображениями. *Современные проблемы дистанционного зондирования Земли из космоса* 2026; 23(1): 49-62.
- Цыпкин Я.З. *Информационная теория идентификации*. М.: Наука, Физматлит; 1995.
- Tashlinskii A.G., Safina G.L. Synthesis of stochastic algorithm for image registration by the criterion of maximum mutual information. *Computer Optics* 2024; 48(1): 109-117.
- Tashlinskii A.G., Safina G.L., Voronov S.V. Pseudogradient optimization of objective function in estimation of geometric interframe image deformations. *Pattern Recognition and Image Analysis* 2012; 22(2): 386-392.
- Gonzalez R.C, Woods E. *Digital image processing*, 4th ed. New York: Pearson Publisher; 2017.
- Snyder J.P. *Map Projections – A Working Manual*. Washington: U.S. Government Printing Office; 1987.
- Wolf P.R, Dewitt B.A., Wilkinson B. *Elements of Photogrammetry with Applications in GIS*, 4th ed. McGraw-Hill Education; 2014.

Морозов В.П. Курс сферической геодезии. 2-е изд., перераб. и доп. М.: Недра; 1979.

Konecny G. Geoinformation: Remote Sensing, Photogrammetry and Geographic Information Systems, 2nd ed. CRC Press; 2014.

Hill L.L. Georeferencing: The Geographic Associations of Information. MIT Press; 2006.

Zhao H, Zhang B, Wu Ch, Zuo Zh. Development of a Coordinate Transformation method for direct georeferencing in map projection frames ISPRS Journal of Photogrammetry and Remote Sensing 2013; 75: 8–21.

REAL-TIME PREPROCESSING OF A SERIES OF UAV IMAGES FOR THEIR COMBINATION WITH SATELLITE IMAGES

Tashlinskii A.G., Belov A.A.

Ulyanovsk State Technical University

A method for real-time merging of multiple images sequentially acquired from a UAV camera is proposed, with simultaneous compensation for their mutual projective distortions and conversion to the EPSG:3395 geographic coordinate system. The method is aimed at subsequent spatial referencing of the combined aerial images to satellite images for their joint processing. UAV camera image merging is based on a recurrent pseudogradient procedure, which allows for high performance and operability under conditions of a priori uncertainty. The combined images are converted to the EPSG:3395 geographic coordinate system. Software was developed in C++ using the open-source OpenCV library, confirming the effectiveness of the method on real sequences of images from UAV cameras. The software implementation was ported to Raspberry and Radxa single-board computers, whose operation was tested in real time onboard a UAV.



студ. Артемьев Д.Д., доц. Витязев С.В.

Рязанский государственный радиотехнический университет им. В.Ф. Уткина

В работе рассматривается задача идентификации человека по биологическим параметрам функционирования организма. В качестве уникальной характеристики, позволяющей провести идентификацию, используется сердцебиение, причем в качестве датчика сигнала сердцебиения используется радар. Проводится анализ возможности такой идентификации на основе экспериментального стенда, позволяющего регистрировать реальные сигналы. На примере набора записей обсуждаются возможные подходы к решению указанной задачи. Приводятся характеристики, демонстрирующие успешное решение задачи идентификации в рассматриваемых примерах.

Введение

Задача идентификации человека заключается в том, чтобы техническая система могла в автоматическом режиме достоверно и однозначно определять личность человека, выступающего в качестве ее текущего пользователя. Необходимость идентификации возникает во многих случаях, включая ограничение доступа к объектам и устройствам; учет рабочего времени; проверки личности в финансовых организациях; мониторинг состояния оператора и многие другие. Традиционными способами идентификации человека являются распознавание отпечатков пальцев, распознавание лиц, идентификация по радужной оболочке глаза. Относительно новыми источниками информации для идентификации стали форма ушной раковины человека и уникальный характер сердцебиения [1].

Идентификация по сердцебиению оказывается возможной, благодаря множеству факторов, влияющих на характер сердцебиения, набор которых уникален для каждого человека, в том числе расположение и размеры сердца, патологии и особенности функционирования организма. При этом сердцебиение сложно подделать или скрыть.

Стандартным источником информации о характере сердцебиения является электрокардиограмма (ЭКГ). На ЭКГ сердцебиение представляется последовательностью так называемых PQRS-комплексов, рисунок которых является уникальным для каждого человека. Снятие ЭКГ, однако, требует специальных действий, связанных с расположением человека и установкой электродов, что ограничивает применение данного подхода. Целесообразным представляется применением других, желательно бесконтактных, способов регистрации сигналов сердцебиения. Одним из таких способов является применение радиолокационного датчика. В последние годы опубликовано достаточно много работ на эту тему [2-7], однако, достоинства такого подхода наталкиваются на большое число проблем, обусловленных тем, что радиолокационный сигнал, отраженный от грудной клетки человека, с учетом мешающих факторов движения, дыхания и одежды является слабым и скрытым множеством шумов и помех. Поэтому исследования в данной области продолжаются и являются актуальными.

Данная работа посвящена разработке стенда для проведения экспериментов, связанных с регистрацией реальных сигналов и анализу их компонентов, позволяющих проводить идентификацию человека. Основной вопрос, поднимаемый в работе: что из себя представляет сигнал сердцебиения, зарегистрированный радиолокационным датчиком, а не с помощью ЭКГ? Ответ на этот вопрос важен и позволяет говорить о возможности идентификации и алгоритмах, способных повышать ее достоверность.

Стенд регистрации сигналов

В течение последних десяти лет появился целый ряд отладочных модулей на базе радиолокационных датчиков информации, позволяющих проводить широкий спектр экспериментов и стимулирующих активное проникновение радиолокационных технологий в сферу бытового и промышленного применения, в том числе, для решения задач, мониторинга состояния здоровья людей и их перемещения; контроля качества работы промышленных установок; охраны территорий и других задач. В частности, в печати активно публикуются исследования с применением модулей регистрации и обработки радиолокационных сигналов, рассмотренных в [8]. Данный модуль представляет собой FMCW-радар (радиолокатор с непрерывным излучением, использующий частотную модуляцию – Frequency Modulated Continuous Wave). Рабочая частота радара составляет 77 ГГц при ширине полосы до 4 ГГц и разрешением по дальности до 4 см. На модуле размещено две передающие и четыре приемные антенны, что позволяет работать в режиме MIMO (много входов – много выходов – Multiple Input – Multiple Output), комбинируя прием сигнала четырьмя антеннами от первой передающей антенны и прием сигнала четырьмя антеннами от второй передающей антенны, имитируя тем самым наличие восьми приемных каналов, позволяя обеспечить угловое азимутальное

разрешение менее 15 градусов. Данный модуль был использован в работе для записи реальных сигналов и их анализа.

Записи сигналов производились для трех человек на расстоянии 40 см. Время записи каждого сигнала составляло 20 секунд. Записи для разных людей чередовались, чтобы посадка человека и другие факторы не были приняты за отличительные особенности сердцебиения.

Общий вид стенда показан на рисунке 1. Радиолокационный датчик подключен к персональному компьютеру, который производит управление датчиком, запись сигналов и используется для дальнейшего анализа записей.

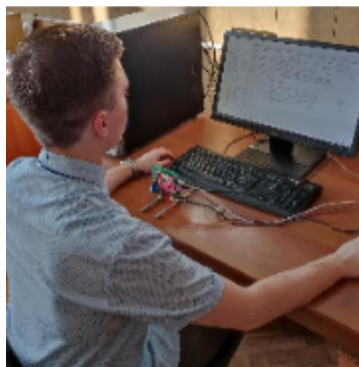


Рисунок 1 – Радиолокационный датчик и запись сигналов

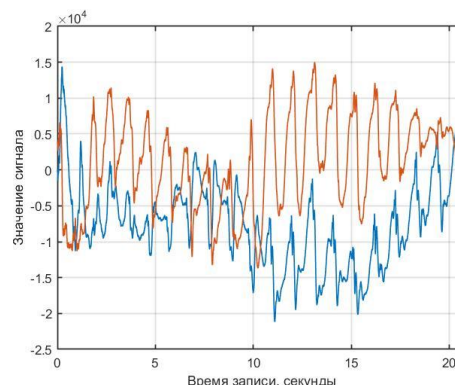


Рисунок 2 – Сигнал на входе в заданном канале дальности – действительная (синий цвет) и мнимая (красный цвет) части

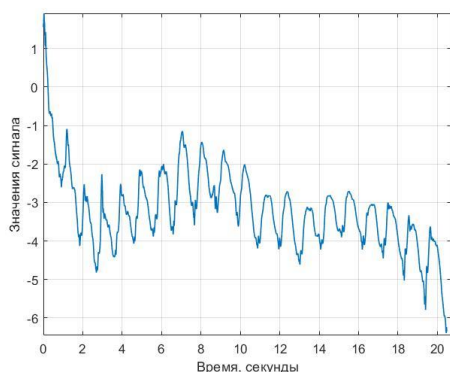


Рисунок 3 – Сигнал сердцебиения – результат выделения фазы с разворачиванием на границах интервала 2π

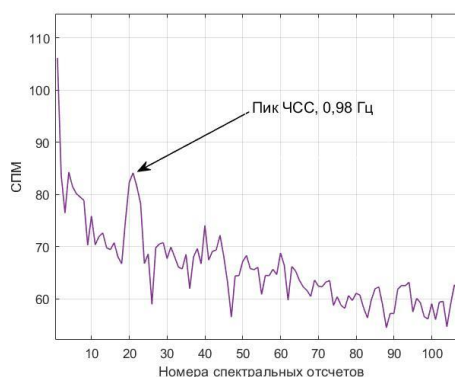


Рисунок 4 – Спектр сигнала сердцебиения

«Сырые данные», поступающие непосредственно с модуля, представляют собой колебания на разностных частотах, соответствующих дальностям до источников отражения (принцип работы FMCW-радара [9]). Первая необходимая процедура – это выполнение прямого быстрого преобразования Фурье (БПФ), выполняющего разделение сигналов по каналам дальности. На этом этапе регистрируемые данные преобразуются в последовательность 3-мерных матриц комплексных отсчетов сигналов. Столбцы матриц представляют собой сигнал, распределенный по каналам дальности; строки матриц несут информацию о колебаниях сигнала в одном канале дальности от зондирования к зондированию; третье измерение возникает из-за наличия восьми приемных каналов (антенная решетка); последовательность матриц используется, поскольку размер одной такой матрицы ограничен объемом внутренней памяти процессора, и для записи 20 секунд его оказывается недостаточно. В рассматриваемой задаче объект – грудная клетка человека – несмотря на колебания, не выходит за пределы одного канала дальности. Поэтому в дальнейшем для анализа следует выделить только канал дальности, соответствующий заданному расстоянию – 40 см. Вид такого сигнала (действительная и мнимая части) показан на Рисунке 1. Математическое описание сигнала представим формулами (1) и (2):

$$s_{in}(t) = A(t) \cdot e^{j\varphi(t)} \quad (1)$$

$$\varphi(t) = \varphi_h(t) + \varphi_r(t) + \varphi_m(t) + \varphi_n(t) \quad (2)$$

В представленных выражениях $A(t)$ – это амплитуда сигнала, не несущая важной информации в рассматриваемой задаче, зависящая от отражающей способности объекта и случайных факторов:

$$A(t) = A_0 + a_n(t) \quad (3)$$

Основная информация в данном случае заключена в фазе сигнала. В результате отражения сигнала от грудной клетки человека и возвращении на приемную антенну фаза поступающего сигнала оказывается в прямой зависимости от расстояния $R(t)$ до грудной клетки (с учетом прямого и обратного пути):

$$\varphi(t) = 2 \cdot \frac{2\pi}{\lambda} \cdot R(t) \quad (4)$$

Поскольку, как было указано выше, частота сигнала составляет около 77 Гц, его длина волны оказывает около 4 мм и колебания грудной клетки, составляющие несколько миллиметров, ощутимо сдвигают фазу сигнала, что и используется для преобразования радиолокационного сигнала в сигнал сердцебиения. В выражении (2) $\varphi_h(t)$ – это составляющая фазы, обусловленная сердцебиением; $\varphi_r(t)$ – составляющая, возникающая из-за дыхания; $\varphi_m(t)$ – соответствует иным колебаниям тела человека, которые всегда есть, даже, если он старается сидеть неподвижно; наконец $\varphi_n(t)$ – случайная составляющая фазы. Входной сигнал для одного из примеров реальной записи представлен на Рисунке 2 (действительная и мнимая части), а его спектр – на Рисунке 3. Важно отметить, что для исследований сердцебиения в этом и последующих примерах записи выполнялись с задержкой дыхания, чтобы минимизировать мешающие факторы.

Интересно, что в самом сигнале (1), судя по Рисунку 2, содержится информация о сердцебиении, хотя основным носителем данной информации должна выступать фаза сигнала. Это можно объяснить тем, что при удалении и приближении грудной клетки мощность обратного рассеяния то уменьшается, то увеличивается, и сигнал изменяет свою амплитуду. Однако более ярко выраженным сигнал сердцебиения должен быть при переходе к фазе сигнала особенно в условиях мешающих воздействий дыхания и других. Переход к фазе можно сделать простым взятием аргумента каждого комплексного отсчета:

$$s_{ph}(t) = \varphi(t) = \arg\{s_{in}(t)\} = \arctg\left(\frac{\operatorname{Im}\{s_{in}(t)\}}{\operatorname{Re}\{s_{in}(t)\}}\right) \quad (5)$$

Сигнал фазы и его спектр показаны на рисунках 3 и 4 соответственно. К сигналу применено «разворачивание» фазы, сохраняющее плавность сигнала на границах диапазона 2π .

Таким образом, мы описали процесс формирования сигналов сердцебиения, формируемых радиолокационным датчиком. Постараемся теперь проанализировать закономерности данных сигналов, позволяющие использовать их для задач идентификации.

Анализ сигналов сердцебиения

Для проведения анализа с помощью описанного стенда был записан набор сигналов, состоящий из 8 записей для каждого из 3 человек, выполненных в разное время в одинаковых условиях. Постараемся ответить на следующие вопросы. Первый вопрос: что представляет собой радиолокационный сигнал сердцебиения; второй вопрос: имеют ли специфические отличия такие сигналы, регистрируемые для одного человека?

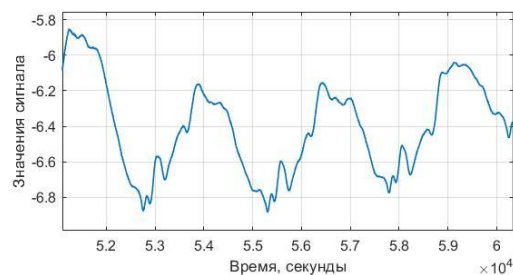


Рисунок 5 – Сигнал 1.1

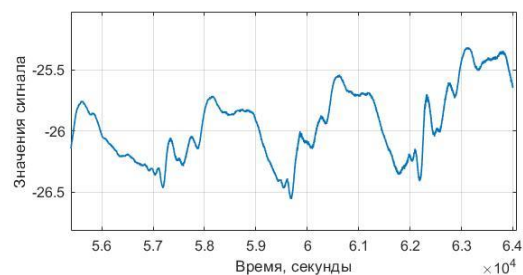


Рисунок 6 – Сигнал 1.2

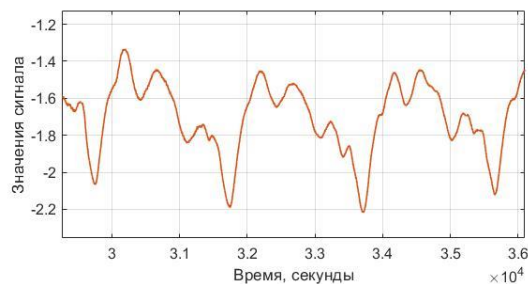


Рисунок 7 – Сигнал 2.1

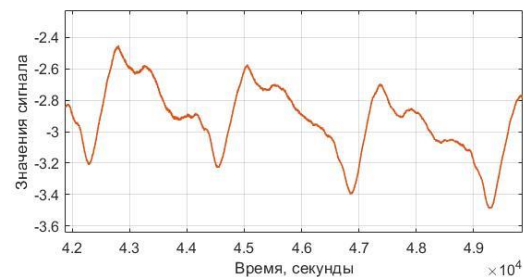


Рисунок 8 – Сигнал 2.2

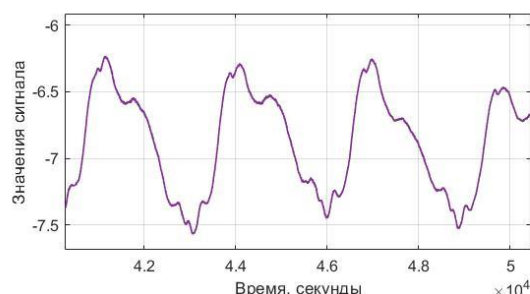


Рисунок 9 – Сигнал 3.1

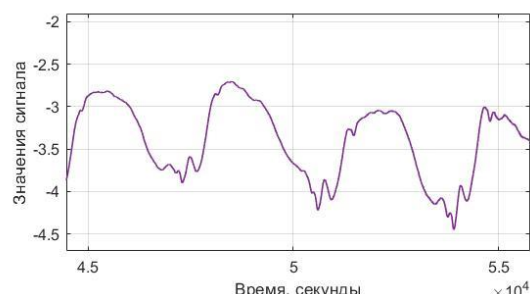


Рисунок 10 – Сигнал 3.2

На рисунках 5-10 показаны сигналы (фрагменты), соответствующие трем людям по две записи для каждого человека (строки – люди; столбцы – первая и вторая записи для каждого человека). Из этих рисунков можно сделать следующие важные выводы.

Во-первых, сигнал сердцебиения, зарегистрированный описанным способом с помощью радиолокационного датчика при достаточной частоте дискретизации (частоте повторения зондирующих импульсов) характеризуется сложной формой, включающей большое количество характерных и неслучайных колебаний, что позволяет говорить о возможной уникальности таких форм и эффективности для использования в целях идентификации человека.

Во-вторых, несмотря на различия рисунков *N.1* и *N.2* очевидны их общие черты и четкие отличия от сигналов, записанных для других людей.

В-третьих, однако, достоверная идентификация требует дополнительных исследований того, какие признаки стоит использовать для идентификации и какие алгоритмы применять для их выделения, а также как сохранить необходимые при идентификации признаки в случаях, когда изменяется вид деятельности человека, поза, одежда и другие факторы.

Заключение

Таким образом, в работе рассмотрена проблема идентификации человека по сигналу сердцебиения, зарегистрированному с помощью радиолокационного датчика. Построен стенд, позволяющий записывать реальные сигналы, и проведен анализ наличия специфических особенностей в радиолокационных сигналах сердцебиения, позволяющих говорить о целесообразности использования данных типов сигналов для задачи идентификации. Показано, что для нескольких человек характер сигналов существенно отличается, потенциально позволяя говорить об эффективности подхода. В то же время необходимо проведение дополнительных исследований для выявления закономерностей, которые позволят обоснованно выбирать структуру решающего устройства и алгоритм обработки сигналов с целью выделения достоверных признаков.

Литература

1. Zheng, G., Li, ZY., Liu, TT., Dai, M. (2011). Study of Human Identification by Electrocardiogram Waveform Morph. In: Sun, Z., Lai, J., Chen, X., Tan, T. (eds) Biometric Recognition. CCB R 2011. Lecture Notes in Computer Science, vol 7098. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25449-9_34.
2. H. Kobayashi, Y. Tanaka and T. Sakamoto, "Individual Identification Using Radar-Measured Respiratory and Heartbeat Features," in IEEE Access, vol. 12, pp. 190972-190987, 2024, doi: 10.1109/ACCESS.2024.3517668.
3. H. Zhao, Y. Ma and X. Wang, "MN-UIV: Multimodal Neural Network Enabling User Identity Verification Based on Millimeter Wave Radar," in IEEE Internet of Things Journal, vol. 11, no. 15, pp. 26304-26313, 1 Aug.1, 2024, doi: 10.1109/JIOT.2024.3395287.
4. M. Alizadeh, G. Shaker, J. C. M. D. Almeida, P. P. Morita and S. Safavi-Naeini, "Remote Monitoring of Human Vital Signs Using mm-Wave FMCW Radar," in IEEE Access, vol. 7, pp. 54958-54968, 2019, doi: 10.1109/ACCESS.2019.2912956.
5. K. Liu, M. Bouazizi, Z. Xing and T. Ohtsuki, "A Comparative Study of Methods of Person Identification Using Radar-Extracted Heartbeat Signals," in IEEE Access, vol. 12, pp. 152196-152211, 2024, doi: 10.1109/ACCESS.2024.3478814.
6. Y. Wang, T. Gu, T. H. Luan, M. Lyu and Y. Li, "HeartPrint: Exploring a Heartbeat-Based Multiuser Authentication With Single mmWave Radar," in IEEE Internet of Things Journal, vol. 9, no. 24, pp. 25324-25336, 15 Dec.15, 2022, doi: 10.1109/JIOT.2022.3196143.
7. T. Sakamoto, "Beyond Contact: The Rise of Wireless Human Sensing Technologies," 2025 Asia-Pacific Microwave Conference (APMC), Jeju, Korea, Republic of, 2025, pp. 1-3, doi: 10.1109/APMC65046.2025.11376689.
8. Texas Instruments, "AWR1642 Evaluation Module (AWR1642BOOST) Single-Chip mmWave Sensing Solution User's Guide," SWRU508B, May 2017, Revised April 2018.
9. X. Li, X. Wang, Q. Yang and S. Fu, "Signal Processing for TDM MIMO FMCW Millimeter-Wave Radar Sensors," in IEEE Access, vol. 9, pp. 167959-167971, 2021, doi: 10.1109/ACCESS.2021.3137387.

ANALYSIS OF HEARTBEAT SIGNALS RECORDED BY A RADAR SENSOR TO SOLVING THE PROBLEM OF HUMAN IDENTIFICATION

stud. Artemyev D.D., assoc. prof. Vityazev S.V.

Ryazan State Radio Engineering University named after V.F. Utkin

The paper examines the problem of identifying a person based on the biological parameters of the functioning of the body. The heartbeat is used as a unique identification feature, using radar as the sensor for the heartbeat signal. An analysis of the possibility of such identification is carried out on the basis of an experimental stand that allows recording real signals. Possible approaches to solving this problem are discussed using a set of records as an example. Characteristics are given that demonstrate the successful solution of the identification problem in the examples under consideration.



НЕЙРОСЕТЕВАЯ СХЕМА ПОСТРОЕНИЯ АЛГОРИТМОВ БПФ

д.т.н., проф. Дорогов А.Ю.^{1,2}¹ПАО «Информационные телекоммуникационные технологии» («Интелтех»),²Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

В работе предложена нейросетевая схема построения алгоритмов быстрого преобразования Фурье (БПФ), основанная на стратификации модели БПФ на топологическую и параметрическую составляющие. Топология определяет граф алгоритма, её выбор инвариантен к виду преобразования и выполняется независимо, следуя правилами проектирования структуры самоподобных нейронных сетей. Выбор параметров базовых операций подчинён топологической модели, и не требует использования итерационных процедур связанных с последовательным разложением дискретных функций Фурье. В результате сложность проектирования алгоритма БПФ не зависит от значения и композиционного представления размерности преобразования. Более того, можно подобрать топологию алгоритма, которая обеспечивает естественную упорядоченность выходных спектральных коэффициентов алгоритма БПФ по частотам следования. В работе приведены примеры построения топологии и БПФ для композиционной размерности.

1. ВВЕДЕНИЕ

Спектральный анализ сигналов, основанный на методах дискретного преобразования Фурье (ДПФ), широко применяется для обработки сигналов в различных областях знаний и технических приложениях. Мощный импульс развития это направление получило после публикации в 1965 году статьи Кули и Тьюки по быстрому преобразованию Фурье (БПФ) [1]. Отчасти этому способствовало бурное развитие вычислительной техники в то время. Следует отметить, что быстрое преобразование Фурье имеет давнюю историю [2]. Первые работы по БПФ, относящиеся к 1805 году, связаны с именем Гаусса [3], но были опубликованы только в 1866 году уже после его смерти. Далее в 19-ом и 20-м веке метод БПФ неоднократно переоткрывался с различными модификациями. В частности, статье Кули и Тьюки непосредственно предшествовала замечательная работа Гуда по алгоритму БПФ [4], (1958г.) которая в то время прошла не замеченной.

Алгоритм БПФ основан на рекуррентной мультипликативной декомпозиции комплексной экспоненты, позволяющей свести вычисление преобразования ДПФ большой композиционной размерности к малым размерностям ДПФ, вплоть до размерности равной двум и за счёт этого кардинально уменьшить число вычислительных операций. Алгоритм Кули-Тьюки был разработан для преобразований размерности $N = 2^n$, которые рекуррентно за n шагов трансформировались в последовательно-параллельную совокупность ДПФ преобразований размерности 2. Этот процесс эквивалентен разложению (факторизации) матрицы ДПФ размерности N в произведение из n слабо заполненных блочных матриц, где блоками являются ДПФ размерности 2, называемых базовыми операциями. Графический образ такой базовой операции напоминает «бабочку», этот термин прижился для алгоритмов данного класса. Схема построения алгоритма БПФ для размерности $N = 2^n$ была проста, наглядна и получила большое распространение. Однако, такая размерность часто избыточна в практических приложениях.

Алгоритм БПФ можно построить и когда размерность преобразования представляет собой некоторую мультипликативную композицию произвольных целых чисел $N = p_0 p_1 \cdots p_{n-1}$, но использование схемы Кули-Тьюки в этом случае становится очень громоздким. Тем не менее, алгоритмические трудности были преодолены, примером является широко-распространённый программный пакет FFTW [5].

Второй особенностью БПФ алгоритмов Кули-Тьюки является необходимость двоично-инверсного переупорядочивания спектральных коэффициентов, для того чтобы привести их последовательность к естественному порядку по возрастанию частоты. Для БПФ размерности $N = p_0 p_1 \cdots p_{n-1}$ принцип переупорядочивания существенно усложняется.

Все известные к настоящему времени схемы построения алгоритмов БПФ имеют отправной точкой базовые функции ДПФ. В результате рекуррентного процесса факторизации системы базовых функций, определяется топологический граф алгоритма БПФ, и одновременно находятся параметры базовых операций. В настоящей работе предлагается разделить эти два процесса. Стратификация процедуры даёт преимущества независимого проектирования и выбора топологии и параметрической настройки базовых операций для выбранной топологии. Этот принцип существенно упрощает способ построения БПФ и открывает возможности его использования для других видов спектральных преобразований. Процедура становится подобной настройке нейронной сети с заданной структурой к выбранной системе базовых функций. Первым шагом в этой процедуре является выбор топологической модели преобразования. Модель должна соответствовать внутренней структуре быстрого алгоритма. Характерным свойством рекуррентных процессов является самоподобие. Методы построения самоподобных многослойных нейросетевых структур

были рассмотрены автором в работах [6,7,8]. С позиций нейросетевой технологии базовые операции быстрого алгоритма уместно назвать нейронными ядрами.

2. НЕЙРОСЕТЕВЫЕ МОДЕЛИ БЫСТРЫХ ПРЕОБРАЗОВАНИЙ

На рисунке 1 в двух вариантах показан пример графа топологической модели самоподобной нейронной сети размерностью 24 при композиции $p_0 = 2, p_1 = 3, p_3 = 4$. Размерность преобразования равна $N = p_0 \cdot p_1 \cdot p_2 = 24$.

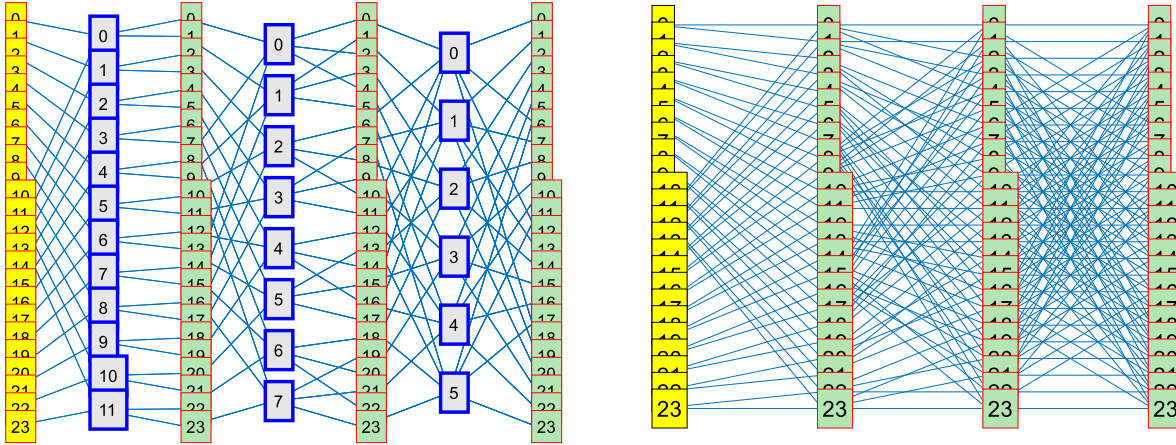


Рисунок 1. Граф топологической модели для БПФ с естественным порядком следования спектральных коэффициентов, вариант 1

Выделенные прямоугольники на графе слева представляют собой базовые операции (нейронные ядра). На графе справа показана та же топологическая модель, но без выделения базовых операций, в этом представлении каждая дуга графа имеет синаптический вес. С точки зрения нейротехнологии, граф представляет собой трёхслойную нейронную сеть с прореженным множеством межслойных связей.

Выбор модели можно подчинить определённым требованиям, например, обеспечить естественный порядок спектральных коэффициентов по частотам следования. На рисунке 1 показан граф топологической модели, обладающий подобным свойством. Топологическая модель имеет аналитическое представление, которое можно записать следующим образом:

$$\begin{aligned} U^m &= \langle u_m u_{m+1} \cdots u_{n-2} u_{n-1} v_{m-1} v_{m-2} \cdots v_1 v_0 \rangle, \\ V^m &= \langle u_{m+1} u_{m+2} \cdots u_{n-1} v_m v_{m-1} v_{m-2} \cdots v_1 v_0 \rangle, \\ z^m &= \langle u_{m+1} \cdots u_{n-2} u_{n-1} v_{m-1} v_{m-2} \cdots v_1 v_0 \rangle. \end{aligned} \quad (1)$$

Здесь индекс $m = 0, 1, \dots, n-1$ – означает номер нейронного слоя (для быстрых преобразований, отсчёт индексов и дискретных переменных принято вести с нуля), $U^m = 0 \cdots (N-1)$ – номер рецептора для слоя m , $V^m = 0 \cdots (N-1)$ – номер аксона для слоя m , z^m – номер нейронного ядра для слоя m , $u_m = 0 \cdots (1-p_m)$ – локальный номер рецептора для ядер слоя m , $v_m = 0 \cdots (1-p_m)$ – локальный номер аксона для ядер слоя m . Числа p_i являются множителями в мультипликативной композиции $N = p_0 p_1 \cdots p_{n-1}$.

Угловые скобки в выражении (1) выделяют кортеж, представляющий число в многоосновной системе счисления. Старшим считается крайний разряд слева, младшим – крайний разряд справа. Аналитическое описание топологической модели достаточно для построения графа алгоритма быстрого преобразования [6]. Графу алгоритма соответствует факторизованное представление матричного преобразования ДПФ, которое имеет вид:

$$H = H_0 H_1 \cdots H_{n-1},$$

где каждой слабозаполненной матрице H_i соответствует один слой графа топологической модели. В работе [7] показано, что для самоподобных сетей элементы матрицы преобразования $H = \|h(U, V)\|$ могут быть выражены в виде произведений элементов матриц базовых операций:

$$h(U, V) = w_{z^{n-1}}^{n-1}(u_{n-1}, v_{n-1}) w_{z^{n-2}}^{n-2}(u_{n-2}, v_{n-2}) \cdots w_{z^0}^0(u_0, v_0). \quad (3)$$

Для преобразования Фурье этот результат был получен Гудом в работе [4].

3. НАСТРОЙКА БЫСТРОЙ НЕЙРОННОЙ СЕТИ НА БАЗИС ФУРЬЕ

По определению, функции дискретного базиса Фурье задаются выражением:

$$F_N(U, V) = \frac{1}{\sqrt{N}} \exp\left(-j \frac{2\pi}{N} UV\right), \quad (4)$$

где U – временной отсчет; V – частота (или номер) базисной функции; $j = \sqrt{-1}$, $N = p_0 p_1 \dots p_{k-1}$ – размерность преобразования (для быстрых преобразований размерность всегда является составным числом). Предполагается, что преобразование ДПФ выполняется как умножение вектора-строки слева на матрицу F_N . Это же правило в дальнейшем будет применяться и к алгоритмам БПФ, по той причине, что оно соответствует направленности графа слева направо по выполняемым операциям. Далее в статье будут рассмотрены два варианта построения алгоритмов БПФ с естественным упорядочением спектральных коэффициентов по частотам следования.

Вариант 1. Для построения алгоритма воспользуемся топологической моделью (1). Полагая $m = 0$ для входного слоя, будем иметь:

$$U = U^0 = \langle u_0 u_1 \dots u_{n-2} u_{n-1} \rangle = \sum_{m=0}^{n-1} u_m p_{m+1} p_{m+2} \dots p_{n-1}.$$

Подставив последнее выражение в (4), и учитывая, что $N = p_0 p_1 \dots p_{n-1}$ получим:

$$F(U, V) = \prod_{m=0}^{n-1} \frac{1}{\sqrt{p_m}} \exp\left(-j \frac{2\pi V}{p_0 p_1 \dots p_m} u_m\right). \quad (5)$$

Для выходного слоя $m = n-1$ из выражения (1) следует:

$$V = V^{n-1} = \langle v_{n-1} v_{n-2} v_{n-3} \dots v_1 v_0 \rangle.$$

Для любого промежуточного разряда с номером m , последнее выражение можно записать в виде:

$$V = \langle v_{n-1} v_{n-2} v_{n-3} \dots v_1 v_0 \rangle = \langle v_{n-1} v_{n-2} \dots v_{m+1} \rangle p_m p_{m-1} \dots p_0 + \dots + v_m p_{m-1} p_{m-2} \dots p_0 + \langle v_{m-1} v_{m-2} \dots v_0 \rangle.$$

Подставляя это выражение в (5) и учитывая периодичность комплексной экспоненты по периоду 2π , после преобразований, получим:

$$F(U, V) = \prod_{m=0}^{n-1} \frac{1}{\sqrt{p_m}} \exp\left(-j 2\pi \left[\frac{u_m v_m}{p_m} + u_m \frac{\langle v_{m-1} v_{m-2} \dots v_0 \rangle}{p_0 p_1 \dots p_m} \right]\right).$$

Каждый сомножитель в этом произведении соответствует элементу базовой операции в мультипликативном представлении (3). Таким образом, получено, что базовые операции алгоритма БПФ определяются выражением:

$$w_{z^m}^m(u_m, v_m) = \frac{1}{\sqrt{p_m}} \exp\left(-j \frac{2\pi}{p_m} u_m v_m\right) \exp\left(-j 2\pi u_m \frac{\langle v_{m-1} v_{m-2} \dots v_0 \rangle}{p_0 p_1 \dots p_m}\right).$$

Кроме разрядных переменных $v_{m-1}, v_{m-2}, \dots, v_0$ выражение для номера ядра z^m содержит переменные $u_{m+1}, \dots, u_{n-2}, u_{n-1}$, это означает, что базовые операции в пределах слоя будут повторяться.

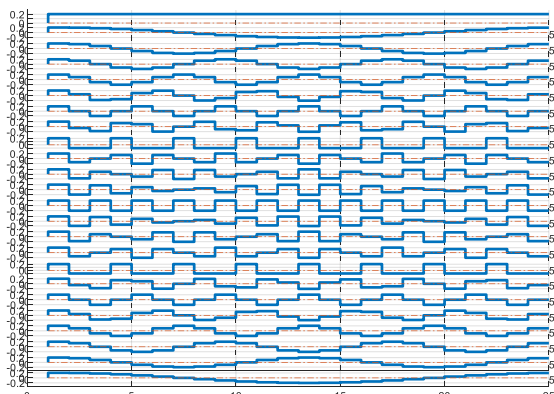


Рисунок 2. Вещественная составляющая базиса Фурье

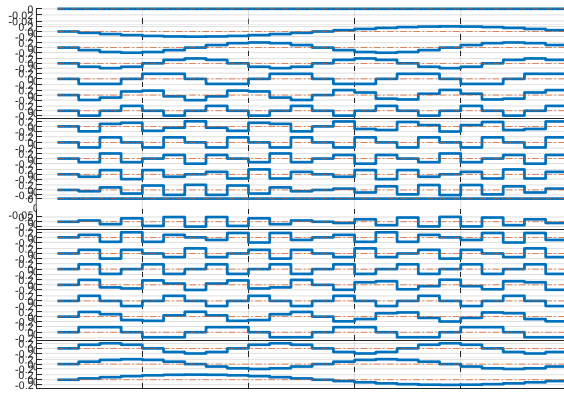


Рисунок 3. Мнимая составляющая базиса Фурье

Следуя выражению (3), по элементам базовых операций, можно восстановить матрицу H дискретного преобразования Фурье. На рисунках 2 и 3 показаны функции, отвечающие столбцам восстановленной матрицы ДПФ для быстрого алгоритма представленного на рисунке 1. Нетрудно видеть, что функции построенного преобразования упорядочены по возрастанию частот.

Вариант 2. Если иначе представить переменные U и V модели, то можно, получить другое выражение для вычисления элементов нейронных ядер. Для координат выходного слоя можно записать:

$$V = V^{n-1} = \langle v_{n-1} v_{n-2} v_{n-3} \cdots v_1 v_0 \rangle = \sum_{m=0}^{n-1} v_m p_{m-1} p_{m-2} \cdots p_0.$$

Подставляя это представление в (4) получим:

$$F(U, V) = \prod_{m=0}^{n-1} \frac{1}{\sqrt{p_m}} \exp \left(-j \frac{2\pi U}{p_m p_{m+1} \cdots p_{n-1}} v_m \right). \quad (6)$$

Для любого m справедливо выражение:

$$U = U^0 = \langle u_0 u_1 \dots u_{n-2} u_{n-1} \rangle = \langle u_0 u_1 \dots u_{m-1} \rangle p_m p_{m+1} \cdots p_{n-1} + \cdots + u_m p_{m+1} p_{m+2} \cdots p_{n-1} + \langle u_{m+1} u_{m+2} \cdots u_{n-1} \rangle.$$

Подставляя последнее в (6) и учитывая периодичность комплексной экспоненты по периоду 2π , после преобразований получим:

$$F(U, V) = \prod_{m=0}^{n-1} \frac{1}{\sqrt{p_m}} \exp \left(-j 2\pi \left[\frac{u_m v_m}{p_m} + v_m \frac{\langle u_{m+1} u_{m+2} \cdots u_{n-1} \rangle}{p_m p_{m+1} \cdots p_{n-1}} \right] \right).$$

Каждый сомножитель в этом произведении соответствует элементу базовой операции в мультипликативном представлении (3). Таким образом, базовые операции алгоритма БПФ определяются выражением:

$$w_{z^m}^m(u_m, v_m) = \frac{1}{\sqrt{p_m}} \exp \left(-j \frac{2\pi}{p_m} u_m v_m \right) \exp \left(-j 2\pi v_m \frac{\langle u_{m+1} u_{m+2} \cdots u_{n-1} \rangle}{p_m p_{m+1} \cdots p_{n-1}} \right).$$

Базовые операции для двух представленных вариантов не совпадают между собой, но соответствуют одной и той же топологической модели. В обоих случаях реализуется БПФ с естественным упорядочением по частотам следования.

4. ЗАКЛЮЧЕНИЕ

В работе предложена нейросетевая схема построения алгоритма быстрого преобразования Фурье. Преимущество предложенной схемы заключается в том, что её сложность сохраняется неизменной независимо от значения и композиционного представления размерности ДПФ преобразования. Новое качество достигается за счёт стратификации модельных представлений на топологическую и параметрическую составляющие. Топологическая модель не зависит от вида преобразования и строится согласно принципам структурного построения самоподобных нейронных сетей [9]. Выбор топологической модели многовариантен, что позволяет учесть дополнительные требования к построению БПФ. В работе предложены топологические модели, которые обеспечивают естественный порядок следования спектральных коэффициентов на выходе алгоритма БПФ по возрастанию частоты. Рассмотренная схема может быть использована для построения быстрых алгоритмов преобразований Уолша-Адамара, Хаара и других подобных ортогональных преобразований.

Литература

1. Cooley, J. W. and Tukey, J. W., "An algorithm for the machine calculation of complex Fourier series," Math. Comput., vol. 19, no. 2, pp. 297-301, April 1965. Reprinted in Digital Signal Processing, I. R. Rabiner and C. M. Rader, Eds., pp.223-227, New York: IEEE Press, 1972.
2. Michael T. Heideman•Don H. Johnson C. Sidney Burrus Gauss and the History of the Fast Fourier Transform IEEE ASSP MAGAZINE october1984, pp. 14-21.
3. Gauss, C. F., 'Nachlass: Theoria interpolationis methodo nova tractata,' pp. 265-303, in earl Friedrich Gauss, Werke, Band 3, Gottingen: Koniglichen Gesellschaft der Wissenschaften, 1866.

4. Good, I. J., "The interaction algorithm and practical Fourier analysis," J. R. Statist. Soc. B, vol. 20, no. 2, pp. 361-372, 1958. Addendum in J. R. Statist. Soc. B, vol. 22, no. 2, pp. 373-375, 1960.
5. Matteo Frigo and Steven G. Johnson The Design and Implementation of FFTW3 Published in Proc. IEEE, vol. 93, no. 2, pp. 216–231 (2005).
6. Дорогов А.Ю. Быстрые преобразования и самоподобные нейронные сети глубокого обучения. Часть 1. Стратифицированные модели самоподобных нейронных сетей и быстрых преобразований. Информационные и математические технологии в науке и управлении. – 2023. – № 4(32). – С. 5-20. – DOI: 10.25729/ESI.2023.32.4.001.
7. Дорогов А.Ю. Быстрые преобразования и самоподобные нейронные сети глубокого обучения. Часть 2. Методы обучения быстрых нейронных сетей. Информационные и математические технологии в науке и управлении.–2024.–№ 1(33).–С.5-19.–DOI:10.25729/ESI.2024.33.1.001.
8. Дорогов А.Ю. Быстрые преобразования и самоподобные нейронные сети глубокого обучения. Часть 3. Пирамидальные нейронные сети с глубокой степенью обучения // Информационные и математические технологии в науке и управлении. – 2024. – № 2(34). – С. 19-32 – DOI:10.25729/ESI.2024.34.2.002 <https://www.imt-journal.ru/archive/public/article?id=366>.
9. Дорогов А. Ю. Самоподобные нейронные сети быстрого обучения / А.Ю. Дорогов. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2024. – 188 с. www.dorogov.su.

NEURAL NETWORK SCHEME FOR BUILDING FFT ALGORITHMS

Prof. Dorogov A.Yu.

St. Petersburg State Electrotechnical University "LETI"
PJSC "Information Telecommunication Technologies" ("Inteltech"), Saint Petersburg

. The paper proposes a neural network scheme for constructing fast Fourier transform (FFT) algorithms based on the stratification of the FFT model into topological and parametric components. The topology defines the graph of the algorithm, its choice is invariant to the type of transformation and is performed independently, following the rules for designing the structure of self-similar neural networks. The choice of the parameters of the basic operations is subordinated to the topological model, and does not require the use of iterative procedures related to the sequential decomposition of discrete Fourier functions. As a result, the complexity of designing the FFT algorithm does not depend on the value and compositional representation of the transformation dimension. Moreover, it is possible to choose the topology of the algorithm, which ensures a natural ordering of the output spectral coefficients of the FFT algorithm by frequencies. The paper provides examples of topology and FFT construction for compositional dimension.



НЕЙРОСЕТЕВАЯ РЕАЛИЗАЦИЯ ПРЕОБРАЗОВАНИЯ КАРУНЕНА-ЛОЭВА

д.т.н., проф. Дорогов А.Ю.^{1,2}

¹ПАО «Информационные телекоммуникационные технологии» («Интелтех»),

²Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»

В работе представлен метод реализации произвольных одномерных и двумерных линейных преобразований в классе самоподобных нейронных сетей, акцент сделан на построение преобразования Карунена-Лоэва. Возможность нейросетевой реализации преобразования позволяет организовать высокоскоростную конвейерную обработку на специализированных процессорах и таким образом снять ограничения по размерности при его использовании. В статье факторизованная форма линейного преобразования рассматривается как многослойная нейронная сеть, а вычисление коэффициентов факторизованной формы как обучение нейронных ядер сети. Алгоритм обучения не имеет обратных связей по ошибке, является абсолютно сходящимся и время его выполнения сопоставимо с временем обработки данных в сети.

5. ВВЕДЕНИЕ

Для задач классификации и распознавания сигналов существенное значение имеют процедуры предварительной обработки, ориентированные на устранение избыточности и выделение информативных признаков. Использование ортогональных преобразований для этих целей позволяет представить информацию, содержащуюся в исходном сигнале в виде взаимно-независимых спектральных составляющих. Поскольку энергия сигнала определяется суммой квадратов спектральных коэффициентов, то по модулю спектрального коэффициента можно непосредственно судить о значимости информативного признака.

Известно, что максимальное сокращение избыточности данных обеспечивается ортогональным преобразованием Карунена-Лоэва, которое образуется собственными векторами ковариационной матрицы сигналов. Преобразование впервые было предложено Хотеллингом [1] позже переоткрыто Каруненом и Лоэвом [2,3]. Однако практическое использование данного преобразования сопряжено со значительными вычислительными затратами, которые квадратично растут с увеличением размерности преобразования. По этой причине метод Карунена-Лоэва в настоящее время не применяется для обработки данных высокой размерности.

Традиционно для обработки сигналов используются ортогональные преобразования, обладающие быстрыми алгоритмами выполнения. Быстрые алгоритмы основаны на возможности факторизации преобразования в произведение слабозаполненных матриц, каждую из которых можно интерпретировать как слой нейронной сети. Факторизация преобразований решает две задачи, во-первых сокращает общее число вычислительных операций и во-вторых позволяет организовать высокоскоростную конвейерную обработку на специализированных процессорах. Общеизвестно, что преобразование Карунена-Лоэва не имеет быстрого алгоритма. Это утверждение действительно справедливо для процессоров последовательного типа, но этот факт не связан с факторизацией. В этой статье будет показано, что факторизация преобразования Карунена-Лоэва возможна, и, следовательно, возможна его быстрое выполнение на специализированных процессорах конвейерного типа.

6. БАЗОВАЯ СХЕМА ФАКТОРИЗАЦИИ БЫСТРЫХ ПРЕОБРАЗОВАНИЙ

В основе построения схемы факторизации лежат классические алгоритмы быстрых преобразований. В работе [4] показано, что они являются частным случаем многослойных самоподобных нейронных сетей. На рисунке 1 представлен граф быстрого преобразования Фурье размерности 8 с топологией Кули-Тьюки «с прореживанием по времени». В каждом слое выделены четыре базовых операции типа «бабочка». Для преобразования Фурье параметры базовых операций полностью определены, однако, если полагать, что их параметры можно изменять, то мы приходим к варианту быстрых нейронных сетей (БНС) [4]. В этом контексте базовые операции уместно назвать нейронными ядрами.

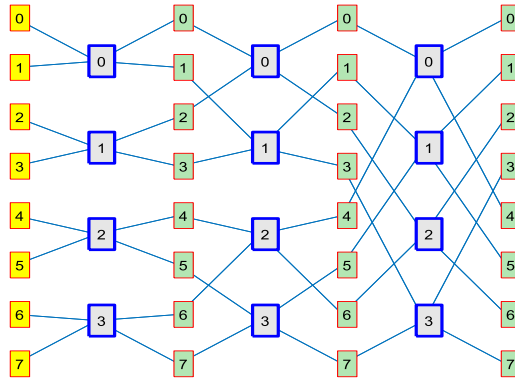


Рисунок 4. Граф быстрого преобразования Фурье

Сетевая модель данной топологии и описывается набором кортежей [4]:

$$\begin{aligned} U^m &= \langle u_{n-1} u_{n-2} \cdots u_{m+1} u_m v_{m-1} v_{m-2} \cdots v_1 v_0 \rangle, \\ V^m &= \langle u_{n-1} u_{n-2} \cdots u_{m+1} v_m v_{m-1} v_{m-2} \cdots v_1 v_0 \rangle, \\ Z^m &= \langle u_{n-1} u_{n-2} \cdots u_{m+1} v_{m-1} v_{m-2} \cdots v_1 v_0 \rangle. \end{aligned} \quad (1)$$

где z^m порядковый номер нейронного ядра, U^m, V^m - порядковые номера рецепторов и аксонов в слое m , u_m, v_m - локальные номера рецепторов и аксонов в пределах ядра слоя m . Каждый кортеж представляет собой поразрядную форму представления порядкового номера через разрядные переменные u_m, v_m . Основания разрядных переменных u_m, v_m определяются целыми положительными числами, и могут быть заданы соответствиями:

$$\begin{pmatrix} u_0 & u_1 & \cdots & u_{n-2} & u_{n-1} \\ p_0 & p_1 & \cdots & p_{n-2} & p_{n-1} \end{pmatrix}, \quad \begin{pmatrix} v_0 & v_1 & \cdots & v_{n-2} & v_{n-1} \\ g_0 & g_1 & \cdots & g_{n-2} & g_{n-1} \end{pmatrix}.$$

Для ядер размерности 2×2 все разрядные переменные принимают значения $\{0,1\}$. Координатные направления U^m и V^m в дальнейшем будем называть входной и выходной плоскостью нейронного слоя. Для терминальных плоскостей (относящихся к начальному и конечному слою сети) будем использовать обозначения U и V . Для построения быстрых алгоритмов размерность преобразования должна быть составным числом и чем больше множителей в разложении размерности, тем выше вычислительная эффективность быстрого алгоритма. Размерности быстрой нейронной сети по входу и выходу вычисляются через произведения оснований разрядных переменных:

$$N = p_{n-1} \cdots p_1 p_0, \quad M = g_{n-1} \cdots g_1 g_0.$$

Число слоёв в быстрых преобразованиях равно числу сомножителей в этих произведениях. Несмотря на большое разнообразие быстрых алгоритмов, конфигурации их структур удовлетворяют системному инварианту самоподобия [4]. Как известно таким же свойством самоподобия обладают фракталы. Поэтому быстрые алгоритмы можно интерпретировать как квазифракталы. Свойство структурной фрактальности позволяет решить одновременно две задачи: реализовать быструю обработку данных и выполнить быстрое обучение преобразования. Обучение быстрого преобразования заключается в выборе значений элементов нейронных ядер, так чтобы в столбцах матрицы преобразования содержался заданный набор опорных функций, это могут быть, например, функции базиса Карунена-Лоэва или другого линейного преобразования. В [4] показано, что для самоподобных нейронных сетей элементы матрицы быстрого преобразования могут быть выражены через произведения элементов нейронных ядер:

$$h(U, V) = w_{z^{n-1}}^{n-1}(u_{n-1}, v_{n-1}) w_{z^{n-2}}^{n-2}(u_{n-2}, v_{n-2}) \cdots w_z^0(u_0, v_0).$$

Там же доказано, что произвольная функция, заданная на дискретном интервале длиной $N = p_{n-1} \cdots p_1 p_0$ также может быть представлена в мультипликативной форме:

$$f(u) = \phi_{i^0}(u_0) \phi_{i^1}(u_1) \cdots \phi_{i^{n-2}}(u_{n-2}) \phi_{i^{n-1}}(u_{n-1}),$$

где $i^m = \langle u_{n-1} u_{n-2} \cdots u_{m+1} \rangle$. Отсюда следует правило настройки нейронных ядер

$$w_{z^m}^m(u_m, v_m) = \phi_{i^m}^k(u_m). \quad (2)$$

Здесь k - номер опорной функции. Зададим точку привязки функции в выходной плоскости числом, представленным в поразрядной форме:

$$x = \langle x_{n-1} x_{n-2} \cdots x_0 \rangle.$$

тогда номера настраиваемых ядер по слоям будет определяться выражением:

$$z^m = \langle u_{n-1} u_{n-2} \cdots u_{m+1} x_{m-1} x_{m-2} \cdots x_1 x_0 \rangle.$$

Для $m = 0$ имеем $z^0 = \langle u_{n-1} u_{n-2} \cdots u_1 \rangle$, это означает, что независимо от выбора точки привязки, все ядра слоя будут настраиваться, причём номер ядра определяется из условия: $z^0 = i^0$. Настройка элементов ядер этого слоя выполняется по правилу:

$$w_{z^0}^0(u_0, v_0) = \phi_{i^0}^k(u_0).$$

Очевидно, должно быть задано взаимно-однозначное соответствие $k \leftrightarrow v_0$ между номером опорной функции k и разрядной переменной v_0 . Эта разрядная переменная принимает значения $0, 1, \dots, g_0 - 1$. Отсюда следует вывод, что число опорных функций не может быть больше чем g_0 , а если ещё потребовать выполнения условия ортогональности ядер, то матрица такого преобразования будет содержать только одну произвольную функцию в качестве столбца. Этого явно недостаточно для реализации произвольного ортогонального базиса Карунена-Лоэва, что согласуется с утверждением об отсутствии быстрого алгоритма для преобразования Карунена-Лоэва. Однако, в следующем разделе будет показано, что отсутствие быстрого алгоритма не препятствует процедуре факторизации преобразования.

7. САМОПОДОБНЫЕ НЕЙРОННЫЕ СЕТИ С ДОПОЛНИТЕЛЬНЫМИ ПЛОСКОСТЯМИ

Дополним топологическую модель быстрого преобразования (1) дополнительными плоскостями нейронных ядер [5], номера которых определим переменной π_m , новая топологическая модель в этом случае будет описываться набором кортежей:

$$\begin{aligned} U^m &= \langle u_{n-1} u_{n-2} \cdots u_{m+1} u_m v_{m-1} v_{m-2} \cdots v_1 v_0 \rangle, \\ V^m &= \langle u_{n-1} u_{n-2} \cdots u_{m+1} v_m v_{m-1} v_{m-2} \cdots v_1 v_0 \rangle, \\ z^m &= \langle u_{n-1} u_{n-2} \cdots u_{m+1} v_{m-1} v_{m-2} \cdots v_1 v_0 \rangle, \\ \pi_m &= \langle v_{n-1} v_{n-2} \cdots v_{m+2} v_{m+1} \rangle. \end{aligned}$$

Максимальное количество дополнительных плоскостей появится в нулевом слое. Номер плоскости в нулевом слое будет определяться кортежем $\pi_0 = \langle v_{n-1} v_{n-2} \cdots v_2 v_1 \rangle$. Плоскость с номером $\pi_0 = 0$ будем считать плоскостью исходной базовой топологической структуры. Число плоскостей в нулевом слое будет равно произведению оснований: $g_{n-1} g_{n-2} \cdots g_2 g_1$. По мере движения к выходному слою число дополнительных плоскостей будет уменьшаться и для последнего слоя $\pi_{n-1} = \langle \rangle$, т.е. их не будет совсем, останется только одна плоскость базовой топологии. Таким образом, в новой топологии плоскость последнего слоя останется прежней, а в младших слоях появятся дополнительные плоскости. Номер ядра, теперь следует уточнять его размещением в дополнительной плоскости. На рисунке 2 показана новая топология, построенная на базе трёхслойной сети с основаниями 2.

В сети условно показаны коммутаторы (SW), которые служат для пояснения принципа работы сети. Коммутаторы управляются разрядными переменными точек выходной плоскости. Фактически коммутаторов нет, они реализуются в составе алгоритма и не препятствуют параллельной обработке входных данных. В контексте спектрального преобразования точки выходной плоскости точки ассоциируются со спектральными коэффициентами, поэтому привязка спектрального коэффициента к координатам выходной плоскости предопределяет выбор дополнительных плоскостей, которые используются для обработки входных образов. При построении полного спектрального анализатора все векторные входы параллельно объединяются.

Поскольку правило порождения новых плоскостей не противоречит базовой топологической модели, то для настройки ядер преобразования к эталону можно использовать прежнее правило (2), расширив его аргументом π_m для дополнительных плоскостей:

$$w_{z^m}^m(\pi_m)(u_m, x_m) = \phi_{i^m}^k(u_m),$$

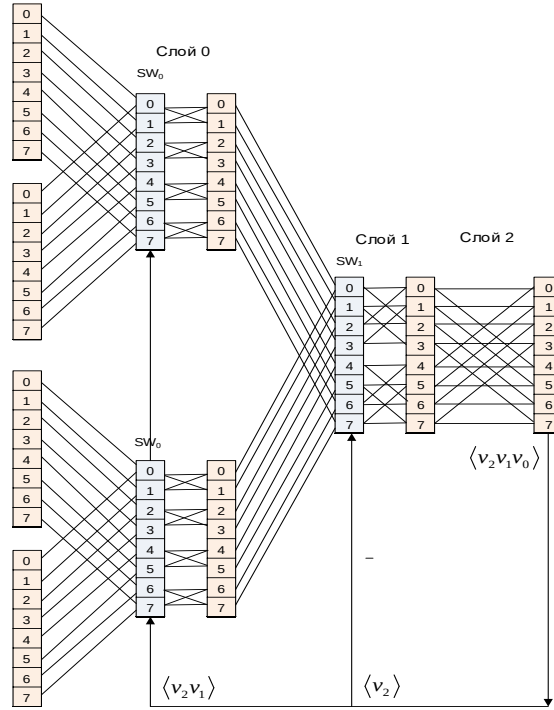


Рисунок 5. Топология самоподобной нейронной сети с дополнительными плоскостями

здесь k - номер эталонной функции, $x = \langle x_{n-1}x_{n-2} \dots x_0 \rangle$, точка привязки, $z^m = \langle u_{n-1}u_{n-2} \dots u_{m+1}x_{m-1}x_{m-2} \dots x_1x_0 \rangle$ номер настраиваемых ядер по слоям, $\pi_m = \langle x_{n-1}x_{n-2} \dots x_{m-1} \rangle$ - номер плоскости размещения ядер. Индекс k в правой части нумерует точку приспособления. Для $m=0$ имеем $z^0 = i^0 = \langle u_{n-1}u_{n-2} \dots u_1 \rangle$, а варьируемыми переменными в левой части являются номер плоскости $\pi_0 = \langle x_{n-1}x_{n-2} \dots x_1 \rangle$ и разряд x_0 . Вместе они покрывают весь диапазон координат выходной плоскости. Этому диапазону отвечают возможные значения индекса k в правой части, отсюда следует, что каждая точка выходной плоскости может быть связана с собственной опорной функцией. Т.е. построенная сеть обладает максимально возможным числом точек привязки, покрывающих всю выходную плоскость и, таким образом может быть использована для реализации произвольного линейного преобразования размерности $N \times M$. В частности, при реализации ортогонального преобразования Карунена-Лоэва для которого выполняется $N = M$.

8. ФАКТОРИЗАЦИЯ ДВУМЕРНЫХ ПРЕОБРАЗОВАНИЙ

Обозначим через $F(U_y, U_x)$ матрицу изображения размером $N_y \times N_x$. При воздействии на изображение линейного преобразования $H(U_y, U_x; V_y, V_x)$ на выходе получается массив из $M_y \times M_x$ коэффициентов.

Необходимым условием существования быстрого алгоритма является возможность мультипликативной декомпозиции значений обоих размерностей изображения в равное число сомножителей:

$$\begin{aligned} N_y &= p_0^y p_1^y \dots p_{n-1}^y, & M_y &= g_0^y g_1^y \dots g_{n-1}^y, \\ N_x &= p_0^x p_1^x \dots p_{n-1}^x, & M_x &= g_0^x g_1^x \dots g_{n-1}^x. \end{aligned}$$

Индексы x, y здесь означают принадлежность к осям координат исходного изображения. Используя сомножители декомпозиций как основания системы счисления, представим значения координат точек изображения в позиционной форме:

$$U_y = \langle u_{n-1}^y u_{n-2}^y \dots u_1^y u_0^y \rangle, \quad U_x = \langle u_{n-1}^x u_{n-2}^x \dots u_1^x u_0^x \rangle.$$

Аналогично можно выразить координаты спектральных коэффициентов в плоскости $[V_y, V_x]$

$$V_y = \langle v_{n-1}^y v_{n-2}^y \dots v_1^y v_0^y \rangle, \quad V_x = \langle v_{n-1}^x v_{n-2}^x \dots v_1^x v_0^x \rangle.$$

Как и в одномерном случае можно доказать [4], что элементы четырехмерной матрицы быстрого преобразования выражаются через элементы нейронных ядер:

$$H(U_y, U_x; V_y, V_x) = W_{z_x^{n-1}, z_y^{n-1}}^{n-1} (u_{n-1}^y u_{n-1}^x; v_{n-1}^y v_{n-1}^x) W_{z_x^{n-2}, z_y^{n-2}}^{n-2} (u_{n-2}^y u_{n-2}^x; v_{n-2}^y v_{n-2}^x) \dots W_{z_x^0, z_y^0}^0 (u_0^y u_0^x; v_0^y v_0^x).$$

Доказывается также, что произвольная двумерная функция, заданная на дискретном поле представима в мультипликативной форме:

$$F(U_y, U_x) = f_{j_{n-1}^y j_{n-1}^x}(u_{n-1}^y, u_{n-1}^x) f_{j_{n-2}^y j_{n-2}^x}(u_{n-2}^y, u_{n-2}^x) \dots f_{j_1^y j_1^x}(u_1^y, u_1^x) f_{j_0^y j_0^x}(u_0^y, u_0^x).$$

Будем использовать прежнюю топологическую модель быстрого преобразования (1), но в двумерном варианте. Нарастим модель дополнительными плоскостями, номера плоскостей в пределах слоя определим правилом:

$$\pi_m = \langle v_{n-1}^x v_{n-2}^x \dots v_{m+1}^x v_{n-1}^y v_{n-2}^y \dots v_{m+1}^y \rangle.$$

Очевидно, что максимальное количество дополнительных плоскостей будет в нулевом слое, а по мере увеличения номера слоя количество дополнительных плоскостей будет уменьшаться, и в последнем слое получим $\pi_{n-1} = \langle \rangle$, т.е. дополнительных плоскостей не будет совсем. Таким образом, в новой топологии плоскость последнего слоя останется прежней, а в младших слоях появятся дополнительные плоскости.

Архитектура сети с дополнительными плоскостями показана на рисунке 3. При выполнении спектральной обработки входное изображение подаётся одновременно на все плоскости входного слоя. Слои сети разделены коммутаторами, которые управляются разрядными переменными координатных чисел выходной плоскости спектральных коэффициентов.

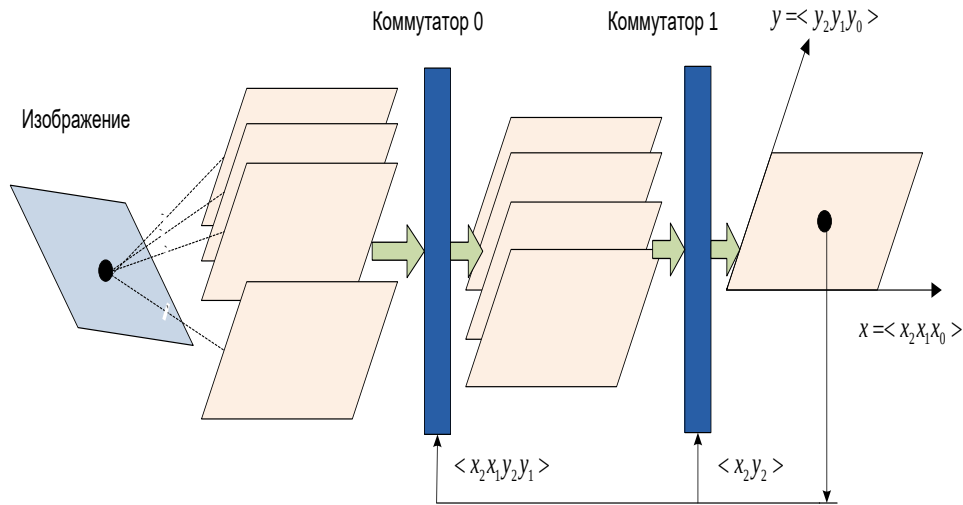


Рисунок 6. Архитектура двумерной регулярной нейронной сети с дополнительными плоскостями

Для настройки ядер преобразования можно использовать правило [4]:

$$W_{z_x^m, z_y^m}^m \langle \pi_m \rangle (u_m^y u_m^x; v_m^y v_m^x) = f_{j_x^m j_y^m}^k (u_m^y, u_m^x).$$

Индекс k в правой части нумерует точку привязки. Для $m=0$ имеем $z_x^0 = j_x^0$ и $z_y^0 = j_y^0$, а варьируемыми переменными в левой части являются разрядные переменные $v_0^y v_0^x$ и номер плоскости $\pi_0 = \langle x_{n-1} x_{n-2} \dots x_1, y_{n-1} y_{n-2} \dots y_1 \rangle$ (здесь разрядные переменные u_*, x_* определяют координаты точки привязки в плоскости $[V_y, V_x]$). Вместе набор варьируемых переменных покрывают весь диапазон координат выходной плоскости. Этому диапазону отвечают возможные значения индекса k в правой части последнего выражения. Таким образом, быстрое преобразование с дополнительными плоскостями может быть настроено к $D = M_y M_x$ произвольным изображениям, т.е. каждой точке выходной плоскости будет соответствовать один опорный образ, например, это может быть образ соответствующий двумерной базисной функции преобразования Карунена-Лоэва.

9. ЗАКЛЮЧЕНИЕ

В статье показано, что топология одномерных и двумерных БНС легко расширяется дополнительными плоскостями, при этом число реализуемых опорных функций кардинально возрастает и покрывает все элементы выходной плоскости. Причём расширение топологии не нарушает принципа построения обучающего алгоритма. Полученные результаты позволяют построить факторизованное представление для любого линейного преобразования, в том числе и для ортогонального преобразования Карунена-Лоэва. Вычислительный эффект от факторизации достигается при использовании специализированных конвейерных вычислителей. Предложенная архитектура реализует сети с глубокой степенью обучения. Можно показать, что они сегментируются в лес независимых пирамидальных сетей [6]. Это порождает уникальное качество – возможность дообучения сети к новым образам без изменения или потери ранее накопленных знаний. Сети

могут работать в системах реального времени, поскольку время обучения не превышает времени обработки данных в сети. Алгоритмы обучения являются абсолютно устойчивыми и завершаются за конечное число шагов. Выбор структуры сети не вызывает проблем и определяется системными инвариантами самоподобных сетей. Возможны различные структурные решения, обладающие одинаковыми свойствами.

10. ЛИТЕРАТУРА

1. Hotelling, H. (1933). Analysis of a complex of statistical variables into principal components. *Journal of Educational Psychology*, 24, 417–441, and 498–520..
2. K. Karhunen, Kari, *Über lineare Methoden in der Wahrscheinlichkeitsrechnung*, *Ann. Acad. Sci. Fennicae. Ser. A. I. Math.-Phys.*, 1947, No. 37, 1-79.
3. Лоев М., *Теория вероятностей*, — М.: ИЛ, 1962.
4. Дорогов А.Ю. *Теория и проектирование быстрых перестраиваемых преобразований и слабосвязанных нейронных сетей*. СПб.: «Политехника», 2014. 328с.
5. Дорогов А.Ю. Быстрые нейронные сети глубокого обучения // III Международная научная конференция по проблемам управления в технических системах (CTS'2019). Сборник докладов. Санкт-Петербург. 30 октября - 1 ноября 2019 г. СПб.: СПбГЭТУ «ЛЭТИ». С. 275-280.
6. Дорогов А.Ю. Быстрые пирамидальные нейронные сети глубокого обучения для адаптивной цифровой обработки сигналов // 78-я Научно-техническая конференция Санкт-Петербургского НТО РЭС им. А.С. Попова, посвящённая Дню радио. Сборник материалов. 2023 СПб.: СПбГЭТУ «ЛЭТИ». с. 107-111. Электронное издание. ISBN 978-5-7629-3183-0.

NEURAL NETWORK IMPLEMENTATION OF THE KARHUNEN-LOEVE TRANSFORMATION

Prof. Dorogov A.Yu.

St. Petersburg State Electrotechnical University "LETI"
PJSC "Information Telecommunication Technologies" ("Inteltech"), Saint Petersburg

The paper presents a method for implementing arbitrary one-dimensional and two-dimensional linear transformations in a class of self-similar neural networks, with an emphasis on constructing the Karhunen-Loeve transform. The possibility of neural network implementation of the transformation makes it possible to organize high-speed pipelining on specialized processors and thus remove dimensional constraints when using it. In the article, the factorized form of a linear transformation is considered as a multilayer neural network, and the calculation of the coefficients of the factorized form is considered as training the neural kernels of the network. The learning algorithm has no feedback by error, is absolutely convergent, and its execution time is comparable to the processing time of data on the network.



НЕЙРОСЕТЕВОЕ ПОДАВЛЕНИЕ НЕОПРЕДЕЛЕННОСТИ ГЕЙЗЕНБЕРГА ПРИ ОЦЕНКЕ МАТЕМАТИЧЕСКОГО ОЖИДАНИЯ РЕАЛЬНЫХ БИОМЕТРИЧЕСКИХ ДАННЫХ ДЛЯ МАЛЫХ ВЫБОРОК С НОРМАЛЬНЫМ И РАВНОМЕРНЫМ ЗАКОНОМ РАСПРЕДЕЛЕНИЯ

д.т.н., проф., Иванов А. И.¹ д.т.н., Малыгина Е. А.²
к.т.н., Банных А. Г.³ преп. Ермакова А. И.³
преп. Филипов И. А.³

¹АО «Пензенский научно-исследовательский электротехнический институт»

²Российский технический университет «МИРЭА»

³Пензенский государственный университет

Активно развивающийся искусственный интеллект открывает новые технологические возможности перед исследователями. Одним из направлений является противодействие эффектам недопустимо низкого доверия к результатам, полученным на малых выборках биометрических данных. Целью статьи является демонстрация того, как можно увеличить размеры малой выборки биометрических данных при вычислении математического ожидания реальных биометрических данных в рамках двух гипотез о нормальном и равномерном распределении данных. Показано, что ошибки оценок математического ожидания трех разных приближений независимы и имеют нормальное распределение значений при двух разных законах распределения. Последнее позволяет повысить точность оценок их простым усреднением. При этом нейросети, повышающие достоверность оценок для нормальных и равномерных данных различаются. Утверждается, что рассмотренная процедура является удобным частным случаем обработки данных. В общем случае, когда нет нормального закона распределений значений ошибок нескольких разных приближений, приходится использовать более сложные нейросетевые конструкции с нелинейным приведением промежуточных данных к нормальному закону. При этом разные нормальные законы должны иметь совпадающие первые моменты: стандартные отклонения и математические ожидания.

Введение

В конце прошлого века в ряде передовых стран начала активно развиваться биометрия [1]. Лидером в биометрических исследованиях являлись США. Первые национальные стандарты по биометрии появились в США. Это лидерство обусловлено тем, что в мире существуют более 160 государственных образований, выдающих своим гражданам международные паспорта с вклеенными в них фотографиями владельцев, имеющие образец автографа владельца или папиллярный рисунок линий отпечатка пальца. Развитие полиграфических технологий облегчает изготовление качественных подделок международных паспортов. Решить проблему защиты от подделки документов на бумажном носителе удастся, вклеим в паспорт микросхему с его электронным дубликатом [1]. В этом случае гарантией подлинности паспорта является электронная цифровая подпись, так как подделать криптографию намного сложнее, чем подделать паспорт на бумажном носителе.

Дополнительной гарантией подлинности паспорта является автоматическая проверка совпадения биометрических данных его владельца в микросхеме и биометрических данных лица его предъявившего. Для стандартизации процедур автоматической проверки биометрии был создан в 2002 году международный технический комитет ISO/IEC JTC1 (Информационные технологии) с подкомитетом - SC37 (Биометрия). С момента своего создания по настоящее время этим техническим подкомитетом создано порядка 150 международных стандартов по биометрической идентификации личности человека.

Параллельно с развитием биометрии практически во всех странах были разработаны и введены в действие законы, существенно ограничивающие права на обработку персональных данных пользователей и в том числе персональных биометрических данных пользователей. В связи с необходимостью выполнения жестких требований по защите обработки персональных биометрических данных появилась необходимость по переходу от процедур биометрической идентификации (сравнения предъявленной биометрии с ее шаблоном) к более сложным процедурам биометрико-криптографической аутентификации. То есть при преобразованиях данных предъявленную пользователем неоднозначную (нечеткую) биометрию следует преобразовать в четкий (однозначный) ключ биометрико-криптографической аутентификации.

При решении задачи биометрико-криптографической аутентификации биометрии зарубежные исследователи пошли по пути применения так называемых «нечетких экстракторов» [2, 3, 4]. Технология «нечетких экстракторов» построена на том, что у всех биометрических данных вычисляется среднее значение. Затем каждый биометрический параметр сравнивается со средним (квантуется). Если параметр выше среднего, то соответствующему разряду «нечеткого» ключа присваивается состояние «1». Если параметр меньше среднего, то его разряду ключа присваивается состояние «0». В итоге получается «нечеткий» ключ, имеющий примерно 30% ошибочных битов. Это очень большое число ошибок. К сожалению, классические коды с обнаружением и исправлением ошибок [5] становятся крайне сложными.

Они плохо правят большое число ошибок. При 50% ошибок классические коды принципиально становятся не работоспособными. Это приводит к тому, что «плохие» не стабильные биометрические данные рисунков отпечатков пальца дают короткие криптографические ключи длиной от 4 до 14 бит [3]. Однако «хорошие» стабильные данные (например, полученные из рисунка радужной оболочки глаза [3]) дают ключ длиной 114 бит, что вполне приемлемо. Как результат, попытки написать международный стандарт [6] по технологии «нечетких экстракторов» провалились.

Одной из причин отсутствия международного стандарта по нечетким экстракторам является то, что на 2014 год выхода в свет работы [6] в России уже был создан пакет национальных стандартов по нейросетевой биометрии. Пакет создавался в рамках работы ТК 362 (Техника защиты информации) в период с 2006 года (ГОСТ Р 52633.0-2006) по 2011 год (ГОСТ Р 52633.5-2011 [7]). Важнейшим преимуществом стандартизованных нейросетевых преобразований является то, что искусственные нейроны перед квантованием биометрических данных выполняют их обогащение. В этом контексте снимается проблема коротких ключей «нечетких экстракторов». При автоматическом обучении нейросети алгоритмом ГОСТ Р 52633.5-2011 [7] длина ключа может быть любой. Каждый нейрон отвечает за один бит ключа. Для длины ключа 256 бит, необходима однослойная нейросеть, состоящая из 256 нейронов. Если биометрические данные «плохие», то их требуется больше (число входов у одного нейрона увеличивается).

Еще одним принципиально важным аспектом стандарта обучения [7] является то, что его реализация требует малых вычислительных ресурсов, например, ресурсов доверенного микропотребляющего контроллера SIM-карты или RFID-карты. Алгоритм автоматического обучения не использует случайный перебор, он детерминированный и выполняет вычисление весовых коэффициентов нейрона, опираясь на математическое ожидание – $E(.)$ и на стандартное отклонение – $\sigma(.)$ конкретного биометрического параметра.

Повышение точность вычислений математического ожидания на малых выборках в 16 примеров с нормальным распределением биометрических данных

Очевидно, что использование малых выборок всегда приводит к ошибкам при вычислении математического ожидания. Оценить то, насколько велика ошибка, из-за ограниченного объема выборки удастся через использование численного моделирования.

Нормальное значение распределения входных данных интересно тем, что две приближенных оценки математического ожидания $E1$ и $E2$ дают итоговое нормальное распределение данных после их нормирования. На рисунке 1 приведены примеры плотностей распределения откликов трех вычисленных приближений математических ожиданий после их нормировки.

Если считать законы распределения рисунка нормальными, то мы можем повысить точность оценки математического ожидания через их усреднение. В результате усреднения стандартное отклонение приближений снижается до величины $\sigma(.) \approx 0.221$. Мы наблюдаем снижение стандартного отклонения на 19.5%. Это эквивалентно повышению объема примеров во входной малой выборке с 16 до 22 (рост на 38%).

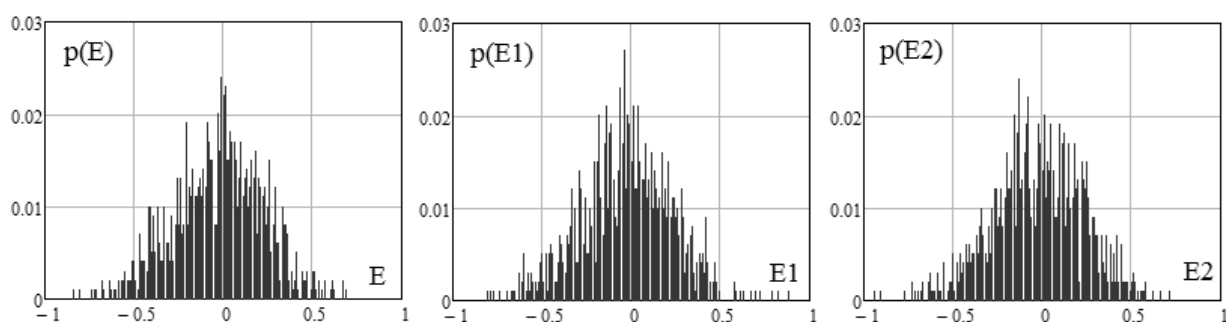


Рисунок 1. Три плотности распределения трех приближенных оценок с нулевым математическим ожиданием со стандартным отклонением $\sigma(.) \approx 0.251$

Таким образом, усреднение трех приближенных оценок математического ожидания малой выборки приводит к эквивалентному росту размеров выборки. Это происходит из-за отсутствия полной зависимости, использованных нами приближений: $\text{corr}(E, E1) \approx 0.643$, $\text{corr}(E, E2) \approx 0.842$, $\text{corr}(E1, E2) \approx 0.33$.

Повышение точность вычислений математического ожидания на малых выборках

Предположительно параллельно со стандартом ГОСТ Р 52633.5-2011 [7] в ближайшее время будет использоваться алгоритм сверхбыстрого автоматического обучения нейронов «на лету» [8]. Этот алгоритм не нуждается в вычислениях весовых коэффициентов и воспроизводит эффект запоминания цыплятами (утятами) образа своих братьев и своей матери. Пользуясь этими знаниями, цыплята и утята строятся друг за другом и идут цепочкой за своей матерью. При этом алгоритм оказывается быстрым и простым из-за того, что естественные нейроны в головах у цыплят и утят заранее (при их формировании в яйце) предобучены различать нормально распределенные данные и равномерно распределенные данные.

Примеры порядка 20 статистических критериев для проверки гипотезы нормального распределения даны в справочнике Кобзаря [9]. В этом же справочнике [9] приведены примерно 20 статистических критериев для проверки гипотезы равномерности распределения данных. И те и другие критерии можно представить искусственными нейронами, предобученными распознавать какое распределение имеет та или иная малая выборка. Примерно 100 вариантов таких предобученных нейронов представлены в справочнике [10]. Все эти 100 вариантов искусственных предобученных нейронов опираются на вычисление математического ожидания по малой выборке.

Как показано выше (рис. 1 и рис. 2) увеличить точность оценки математического ожидания вполне реально за счет обладания предварительной информацией о нормальном распределении данных малой выборки.

Покажем по аналогии, что информация о равномерном распределении данных малой выборки так же может быть использована для повышения точности оценок математического ожидания, что эквивалентно повышению объема малой выборки.

Обе программы используют одинаковые приближения математических ожиданий. Сравнивая их, видим, что приведение данных к одинаковым стандартным отклонениям различны. Весовые коэффициенты у этих программ разные. Тем не менее и для случая равномерного распределения входных данных отклики трех приближений имеют близкие к нормальным распределения, что отображено на рисунке 2.

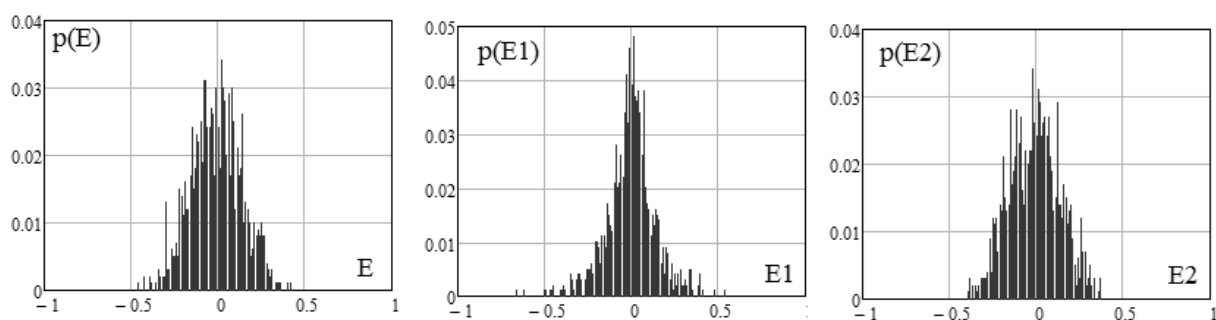


Рисунок 2. Три плотности распределения трех приближенных оценок с нулевым математическим ожиданием с стандартным отклонением $\sigma(.) \approx 0.144$

Воспользовавшись нулевым значением математических ожиданий и равными дисперсиями распределений, мы можем поднять точность вычислений их усреднением. В этом случае наблюдается снижение стандартного отклонения с величины 0.144 до величины 0.121 (на 19%). Это эквивалентно увеличению объема малой выборки с величины в 16 опытов до величины в 22 опыта (рост на 35%). Таким образом, мы наблюдаем возможность существенного увеличения объема малой выборки на 35% или повышения достоверности вычислений. Это эффект использует факт отсутствия полной зависимости, использованных нами приближений: $\text{corr}(E, E1) \approx 0.548$, $\text{corr}(E, E2) \approx 0.888$, $\text{corr}(E1, E2) \approx 0.365$.

Выводы

К сожалению, приведенные выше простые алгоритмы повышения достоверности оценок простым усреднением нескольких приближений, работают только для нормальных и равномерно распределенных входных данных малых выборок. Ряд критериев (ряд нейронов) нельзя объединять (обобщать) столь простым правилом. В частности искусственные нейроны среднего геометрического [11] и среднего гармонического [12] имеют асимметричные распределения их откликов. Для того чтобы их использовать необходимо строить нелинейное преобразования, приводящее их отклики к нормальному закону распределения значений.

Тем не менее, общее правило остается работоспособным. Чем больше приближений используется, тем больше удастся поднять достоверность нейросетевых вычислений. То есть возникает задача синтеза

множества новых статистических критериев [13] для проверки гипотезы нормальности и равномерности законов распределения данных малых выборок.

Литература

1. Болл Руд и др. Руководство по биометрии. / Болл Руд, Коннел Джонатан Х., Панканти Шарат, Ратха Налини К., Сеньор Эндрю У. // Москва: Техносфера, 2007. -368 с., (перевод с английского).
2. Dodis Y., Reyzin L., Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy // Proc. EUROCRYPT, April 13, pages 523-540, 2004.
3. Hao F., Anderson R., Daugman J. Crypto with Biometrics Effectively //IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 9, SEPTEMBER, Page(s):1073 – 1074, 2006.
4. Ramírez-Ruiz J., Pfeiffer C., Nolasco-Flores J. Cryptographic Keys Generation Using FingerCodes. //Advances in Artificial Intelligence - IBERAMIA-SBIA 2006 (LNCS 4140), p. 178-187, 2006
5. Р. Морелос-Сапароса Искусство помехоустойчивого кодирования М.: Техносфера, 2007 г., 320 с.
6. S. Rane, "Standardization of Biometric Template Protection," IEEE MultiMedia, vol. 21, no. 4, pp. 94–99, October 2014.
7. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа»
8. Иванов А.И. Бионика: обучение "на лету" с использованием генетически по-разному предобученных искусственных нейронов // Системы безопасности. 2023 № 4, с. 122-125.
9. Кобзарь А.И. Прикладная математическая статистика. Для инженеров и научных работников. М.: ФИЗМАТЛИТ, 2006 г., 816 с.
10. Иванов А.И. НЕЙРОСЕТЕВОЙ МНОГОКРИТЕРИАЛЬНЫЙ СТАТИСТИЧЕСКИЙ АНАЛИЗ МАЛЫХ ВЫБОРОК. Справочник. // Пенза, 2022. Издательство Пензенского государственного университета, 160 с. ISBN: 978-5-907600-83-6.
11. Перфилов К.А. КРИТЕРИЙ СРЕДНЕГО ГЕОМЕТРИЧЕСКОГО, ИСПОЛЬЗУЕМЫЙ ДЛЯ ПРОВЕРКИ ДОСТОВЕРНОСТИ СТАТИСТИЧЕСКИХ ГИПОТЕЗ РАСПРЕДЕЛЕНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ. Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. Том 9, Пенза-2014, с. 92-93
12. Ахметов Б.С., Иванов А.И., Перфилов К.А., Проценко Е.Д., Пашенко Д.С. ИСПОЛЬЗОВАНИЕ СРЕДНЕГО ГЕОМЕТРИЧЕСКОГО, ОЖИДАЕМОЙ И НАБЛЮДАЕМОЙ ФУНКЦИЙ ВЕРОЯТНОСТИ КАК СТАТИСТИЧЕСКОГО КРИТЕРИЯ ОЦЕНКИ КАЧЕСТВА БИОМЕТРИЧЕСКИХ ДАННЫХ с. 281-283. XX Международный симпозиум «Надежность и качество 2015». Том. 2., 15-18 мая 2015.
- 13.** Банных А.Г. и др. Обзор новых статистических критериев проверки гипотезы нормальности и равномерности распределения данных малых выборок / А.П. Иванов, А.И. Иванов, А.В. Безяев, Е.Н. Куприянов, А.Г. Банных, К.А. Перфилов, В.С. Лукин, К.Н. Савинов, С.А. Полковникова, Ю.И. Серикова, А.Ю. Малыгин //Надежность и качество сложных систем. 2022. N2. С. 33-44.

NEURAL NETWORK SUPPRESSION OF HEISENBERG UNCERTAINTY IN ESTIMATING THE MATHEMATICAL EXPECTATION OF REAL BIOMETRIC DATA FOR SMALL SAMPLES WITH A NORMAL AND UNIFORM DISTRIBUTION LAW.

doctor of technical sciences, professor, Ivanov A. I.¹

doctor of technical sciences, Malygina E. A.²

candidate of technical sciences, Bannykh A. G.³

rev. Ermakova A. I.³

rev. Filipov I. A.³

¹ Penza Scientific Research Electrotechnical Institute

² "MIREA - RTU", Moscow

³ HE "Penza State University"

Actively developing artificial intelligence opens up new technological opportunities for researchers. One of the directions is to counteract the effects of unacceptably low confidence in the results obtained on small samples of biometric data. The purpose of the article is to demonstrate how it is possible to increase the size of a small sample of biometric data when calculating the mathematical expectation of real biometric data within the framework of two hypotheses about the normal and uniform distribution of data. It is shown that the errors in the estimates of the mathematical expectation of three different approximations are independent and have a normal distribution of values under two different distribution laws. The latter makes it possible to increase the accuracy of estimates by simply averaging them. At the same time, neural networks that increase the reliability of estimates for normal and uniform data differ. It is argued that the considered procedure is a convenient special case of data processing. In the general case, when there is no normal law for the distribution of error values of several different approximations, it is necessary to use more complex neural network structures with nonlinear reduction of intermediate data to a normal law. At the same time, different normal laws should have the same first points: standard deviations and mathematical expectations.



АВТОМАТИЗИРОВАННАЯ ГЕНЕРАЦИЯ СИНТЕТИЧЕСКИХ РАДИОЛОКАЦИОННЫХ ИЗОБРАЖЕНИЙ ПРИ РАЗРАБОТКЕ СИСТЕМЫ ГРУППОВОГО ТЕХНИЧЕСКОГО ЗРЕНИЯ АВИАЦИОННОГО БАЗИРОВАНИЯ

в.н.с Кокутин С.Н., инж. Сергиев С.А.

АНО ВО «Университет Иннополис»

В работе представлен подход к созданию автоматизированного конвейера генерации наборов синтетических радиолокационных изображений для обучения нейросетевых моделей, применяемых в системе группового технического зрения авиационного базирования. Разработанная система базируется на модифицированном симуляторе с растеризационным ядром, поддерживающим ввод 3D-моделей наземных объектов и растровых масок с различными типами подстилающих поверхностей. Описана концепция доработки симулятора и реализованная архитектура конвейера. Промежуточные результаты демонстрируют возможность формирования сбалансированных датасетов в объеме, достаточном для массового обучения нейросетевых моделей. Предложенный подход направлен на решение проблемы дефицита реальных размеченных радиолокационных изображений, препятствующей развитию технологий группового технического зрения для радиолокационных систем авиационного базирования.

Введение

Развитие технологий технического зрения в радиодиапазоне на базе беспилотных авиационных систем открывает новые возможности для всепогодного мониторинга земной поверхности, поиска и распознавания объектов в сложных метеоусловиях. Радиолокаторы с синтезированной апертурой (РСА), работающие в X-диапазоне (8-12 ГГц), обеспечивают высокое пространственное разрешение, имеют повышенную чувствительность к микрорельефу и текстурным особенностям объектов, обладают оптимальными массогабаритными характеристиками, что делает их перспективными для размещения на легких беспилотных воздушных судах (БВС) [1], в том числе в составе многопозиционных пространственно-распределенных систем.

Ключевым этапом создания интеллектуальных систем анализа радиолокационных изображений (РЛИ) является формирование репрезентативных обучающих выборок. Однако сбор и разметка реальных радиолокационных данных сопряжены со значительными временными и финансовыми затратами, ограниченной доступностью полигонов, а также сложностью получения точных аннотаций для задач семантической сегментации и обнаружения. В этой связи генерация синтетических РЛИ с контролируемой статистикой и автоматической разметкой представляет собой актуальное направление работ.

Зарубежные исследования в области синтетических данных для РСА демонстрируют растущий интерес к использованию симуляторов (имитаторов) для обучения нейросетей. Так, в работе [2] показано, что предварительное обучение на симулированных данных с последующей донастройкой на реальных выборках позволяет существенно повысить точность распознавания. В работе [3] представлен подход к автоматизированному моделированию синтетических РЛИ наземных транспортных средств с использованием симулятора RaySAR, реализующего метод трассировки лучей, и последующему тестированию алгоритмов распознавания. В отечественной практике вопросы моделирования РЛИ для задач машинного обучения рассматриваются в ряде работ [4, 5], однако основной вектор разработок по-прежнему смещен в сторону имитационного моделирования малоразмерных фрагментов, содержащих одиночные объекты. Кроме того, в отечественных исследованиях слабо представлены системные решения по автоматизированному формированию полноценных и релевантных датасетов для многопозиционных систем авиационного базирования, формирующих разноразмерные РЛИ.

Цель данной работы – разработка концепции и архитектуры автоматизированного конвейера формирования масштабных датасетов синтетических РЛИ для обучения нейросетевых моделей, применяемых в многопозиционной системе группового технического зрения на базе нескольких БВС с малогабаритными бортовыми РСА X-диапазона.

Постановка задачи и исходные данные

Разрабатываемая система группового технического зрения авиационного базирования предназначена для решения двух целевых задач. Первая задача состоит в классификации типов подстилающей поверхности на основе семантической сегментации РЛИ. Эта задача требует не только достаточного и сбалансированного по классам объема эталонных данных, но и разнообразия пространственных конфигураций, поскольку радиолокационный отклик существенно зависит от структуры поверхности и условий наблюдения.

Вторая задача связана с распознаванием наземных объектов на основе разноразмерных РЛИ, получаемых при помощи многопозиционной системы. При этом принципиально важно, чтобы в обучающих данных радиолокационные сцены содержали как сам объект, так и реалистичное естественное окружение, поскольку

в РЛИ целевой отклик определяется не только геометрией объекта, но и взаимодействием с подстилающей поверхностью, углами наблюдения и взаимным расположением элементов сцены.

Исходными данными для генерации синтетических РЛИ служат:

- 1) растровые маски подстилающей поверхности с разрешением, соответствующим масштабу сцены, где каждый пиксель содержит код типа поверхности;
- 2) 3D-модели объектов в CAD форматах, совместимых с графическим конвейером, для которых задан параметр УЭПР (удельная эффективная площадь рассеяния);
- 3) параметры РСА: несущая частота (X-диапазон), полоса сигнала, диаграмма направленности;
- 4) траекторные параметры БВС: высота, скорость, углы наблюдения, база между БВС в многопозиционной группе, направление движения, продолжительность съемки.

Исходная решение, применяемое для генерации синтетических РЛИ

Основой конвейера служит программный симулятор на основе растеризации, разработанный на языке Python и реализующий упрощенную физическую модель формирования РЛИ с учетом геометрии съемки с БВС, а также геометрических эффектов затенения, наложения и перспективных наложений. Такой тип симулятора отличается тем, что формирование РЛИ осуществляется не путем пошагового физического трассирования лучей в полном объеме, а посредством преобразования геометрической модели сцены в пиксельную сетку с использованием аппаратного рендеринга, обеспечивающего расчет геометрических искажений в соответствии с конфигурацией наблюдения [6]. Трассировка лучей обеспечивает высокую физическую точность за счет моделирования распространения электромагнитных волн с учетом многократных отражений, однако вычислительная сложность данного метода ограничивает его применение для массового формирования датасетов [7]. В то же время растеризационный подход обеспечивает более простую реализацию, высокую вычислительную производительность за счет поддержки GPU-вычислений, масштабируемость для многопозиционных конфигураций и удобство интеграции в автоматизированные сценарии формирования данных. Следовательно, для задач предварительного обучения нейросетей и дообучения на ограниченных реальных данных растеризационные симуляторы обеспечивают оптимальный баланс между геометрической реалистичностью и производительностью.

Используемый симулятор поддерживает задание двух или трех приемо-передающих позиций. В частности, предусмотрены полноактивная двухпозиционная схема и схема с двумя передатчиками и одним приемником, что позволяет моделировать различные варианты многопозиционной системы группового технического зрения. В отличие от традиционного подхода к синтезу полной апертуры, реализовано формирование потока радиолокационных кадров с повышенной частотой, приближенной к частоте видеопотока. Это позволяет моделировать динамические сцены с движущимися объектами и обеспечивает совместимость с алгоритмами отслеживания в реальном времени.

Базовая версия программного симулятора, использовавшаяся на начальных этапах исследования, не обладала функционалом, необходимым для формирования представительных обучающих выборок. Основным ограничением являлась архитектура управления, которая предполагала либо индивидуальную загрузку предварительно подготовленных сцен, либо ручной ввод параметров для генерации каждого РЛИ посредством графического интерфейса пользователя (GUI). Кроме того, в системе отсутствовали встроенные механизмы автоматической аннотации изображений. В совокупности указанные недостатки исключали возможность пакетной генерации РЛИ и автоматизированного перебора сценариев, что затрудняло варьирование параметров наблюдения и физических характеристик объектов, необходимое для обеспечения масштабирования процесса обучения и воспроизводимости экспериментов.

Для преодоления указанных ограничений и с целью автоматизации конвейера формирования радиолокационных сцен была проведена доработка программного обеспечения.

Концепция автоматизации конвейера формирования радиолокационных сцен

Автоматизированный конвейер формирования радиолокационных сцен представляет собой последовательность программных этапов, обеспечивающих переход от описания параметров сцены к готовым синтетическим РЛИ. Эта архитектура ориентирована на решение ключевой проблемы создания масштабных обучающих датасетов для систем группового технического зрения – необходимость контролируемой пакетной генерации разнообразных сценариев наблюдения с уровнем точности разметки, недостижимым при сборе реальных данных. Архитектура разработанного конвейера исключает ручное вмешательство на большинстве этапов, фокусируясь на управлении распределением присутствия объектов на сцене и распределением типов подстилающих поверхностей, что позволяет масштабировать формирование данных для задач семантической сегментации и распознавания.

Процесс начинается с генерации входного конфигурационного файла посредством специализированного скрипта. Этот скрипт позволяет пользователю задать диапазоны ключевых параметров сцены, включая размеры области наблюдения и характеристики расположения наземных объектов. Полученный файл служит декларативным описанием сценария, где акцент делается на вариативности: вместо фиксированных значений определяются интервалы, из которых далее случайным образом отбираются итоговые комбинации для формируемой сцены.

Ключевым элементом конвейера выступает комбинатор радиолокационных сцен, который принимает входной конфигурационный файл и преобразует его в структурированное описание готовой сцены. Вначале комбинатор размещает фон для сцены, представленный растровой маской, где каждый пиксель соответствует определенному типу подстилающей поверхности. Следующим этапом загружаются 3D-модели целевых объектов и размещаются на фоновой поверхности с учетом заданных диапазонов поворота, масштаба и других параметров расположения на сцене. Далее задаются параметры РСА и траекторий их носителей. В результате формируется выходной конфигурационный файл, содержащий полную спецификацию генерируемой сцены с параметрами, значения которых определены на основе генератора случайных величин в заданных диапазонах.

Выходной конфигурационный файл передается в программный симулятор формирования РЛИ через унифицированный программный интерфейс (API), обеспечивающий бесшовную интеграцию этапов в рамках единого конвейера. В симуляторе выполняется автоматическая генерация синтетических РЛИ и соответствующей разметки.

На рисунке 1 представлена структурная схема предлагаемого конвейера автоматизированной генерации синтетических РЛИ.

Промежуточные результаты

В рамках модификации симулятора на языке Python были реализованы следующие ключевые доработки:

- 1) разработан специализированный скрипт для генерации входного конфигурационного файла в YAML-формате, вызываемый через интерфейс командной строки (CLI). Разработанный скрипт поддерживает как формирование одиночных РЛИ, так и пакетную их генерацию с различными комбинациями объектов;
- 2) разработан модуль комбинатора объектов на радиолокационной сцене, формирующий выходной конфигурационный файл в YAML-формате на основе параметрических описаний сцены и загруженных 3D-моделей объектов, а также параметров РСА и траекторий БВС;
- 3) в программном симуляторе реализован механизм автоматического формирования аннотаций в виде масок для подстилающих поверхностей и ограничивающих рамок для детектируемых объектов;
- 4) выполнена оптимизация ресурсов и времени выполнения ключевых функций программного симулятора. Повышение производительности было достигнуто за счет последовательного устранения узких мест в вычислительном конвейере – переход к пакетной обработке импульсов и считывание данных с GPU. Реорганизация обмена данными между CPU и GPU на основе объектов пиксельного буфера и постоянного отображения памяти позволила реализовать асинхронный режим работы, исключив простои оборудования. В сочетании с векторизацией вычислений и распараллеливанием операций на CPU это позволило свести к минимуму потери времени на синхронизацию процессов и дублирующее копирование памяти, обеспечив многократный прирост скорости генерации без потери качества синтетических РЛИ.



Рисунок 1 – Конвейер автоматизированной генерации синтетических РЛИ

Структура входного конфигурационного файла включает:

- диапазоны изменения границ сцены по пространственным осям;
- набор параметров УЭПР для соответствующего типа подстилающей поверхности (среднее, стандартное отклонение, минимальное или максимальное значение) или путь к растровым маскам;
- классы моделируемых объектов и диапазоны варьирования их параметров, включая долю покрытия указанным классом площади сцены, ориентацию (поворот), множитель масштаба, степень погружения объекта в подстилающую поверхность, значение УЭПР;
- пути к 3D-моделям объектов.

Растровые маски подстилающей поверхности проецируются на горизонтальную плоскость с явно заданной привязкой к мировым координатам. Размещение на сцене подстилающей поверхности и наземных объектов в комбинаторе происходит в соответствии с заданными правилами. При этом поддерживается иерархическая система классов объектов с механизмом наследования: параметры, не указанные для подкласса, автоматически заимствуются у родительского класса или заменяются значениями по умолчанию. Такой подход позволяет компактно описывать сложные сценарии без избыточного дублирования.

На рисунке 2 приведены примеры разноракурсных синтетических РЛИ в наклонной (Slant) плоскости, полученных в передних зонах обзора бортовых РСА трехпозиционной системы, а также визуализация аннотаций ограничивающими рамками, сформированных для этих РЛИ.

Обсуждение

Полученные результаты подтверждают работоспособность предложенного подхода к автоматизированной генерации синтетических РЛИ и целесообразность его применения для преодоления дефицита радиолокационных датасетов, так как традиционный ручной ввод параметров в симуляторе существенно ограничивает объемы и скорость генерации. Ключевым достижением является переход от ручного прототипирования к масштабируемому конвейеру, способному в сжатые сроки формировать крупные и репрезентативные обучающие выборки. Двухэтапная организация конвейера (комбинатор – симулятор) обеспечивает гибкость, недостижимую при монолитной реализации. Разделение конфигурации сцены и процесса моделирования позволяет с минимальными затратами по времени задавать различные сценарии размещения объектов и переиспользовать их для различных траекторий БВС и режимов РСА.

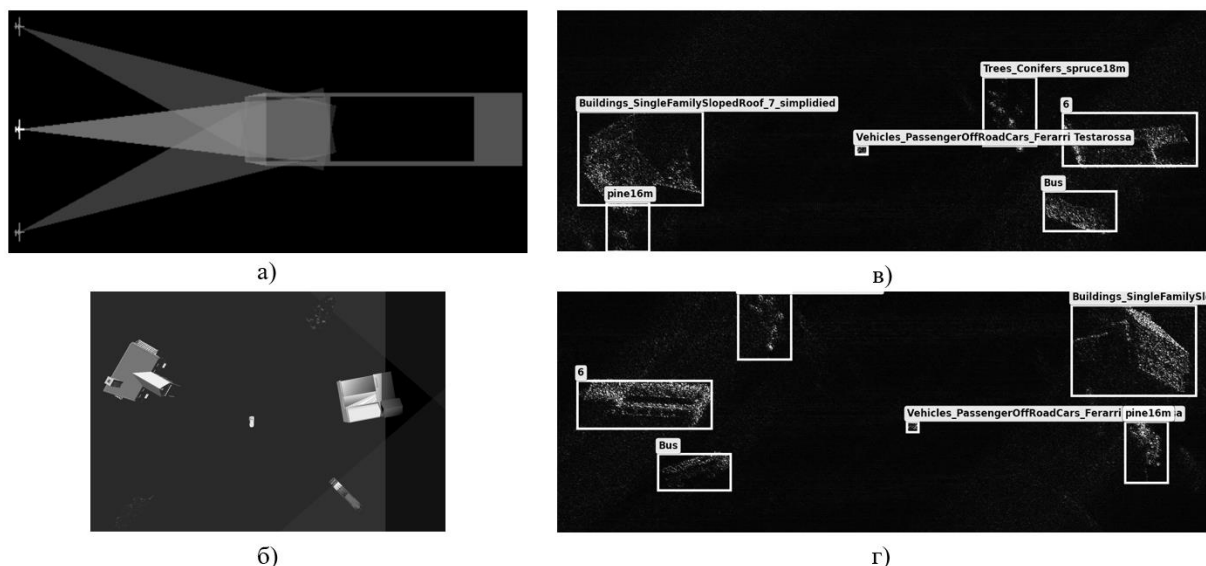


Рисунок 2 – Пример моделирования РЛИ, получаемых в трехпозиционной системе переднего обзора: а) визуализация схемы трехпозиционной бортовой РСА с одной приемной и двумя передающими позициями; б) моделируемая сцена, содержащая наземные объекты 3 классов (здания, транспортные средства, деревья); в) РЛИ, полученное с левого ракурса; г) РЛИ, полученное с правого ракурса

Разработанная логика формирования радиолокационных сцен с заданием диапазонов вариации параметров объектов обеспечивает статистическое разнообразие генерируемых выборок. Автоматическая генерация аннотаций исключает необходимость трудоемкой ручной разметки и снижает риск субъективных ошибок. Использование при моделировании сцен параметров РСА и траекторий их носителей позволяет моделировать многопозиционные сценарии, типичные для группового технического зрения, где несколько радиолокационных платформ наблюдают одну сцену под разными ракурсами.

Вместе с тем проведенный анализ показывает, что для максимально эффективного использования симулятора в составе большого обучающего конвейера требуется дальнейшая доработка по нескольким направлениям.

Первое направление связано с дальнейшим повышением физической реалистичности синтетических РЛИ. Для минимизации ошибок классификации и распознавания необходимо реализовать моделирование адекватных геометрических форм и топологии границ объектов, физически достоверных переходов на границах раздела классов. Для радиолокационной сцены особенно важны тонкие геометрические детали, поскольку именно они формируют характерные радиолокационные признаки и влияют на распознаваемость объектов.

Второе направление вызвано необходимостью формирования крупных и представительных наборов разноракурсных РЛИ, подобных MSTAR и ATRNet-STAR [8], для задач распознавания наземных объектов. Для этого требуется реализовать моделирование траекторного движения носителей в многопозиционной системе с формированием последовательных РЛИ при варьировании в широком диапазоне азимутальных углов и углов места.

Третье направление развития связано с формированием оптимальной структуры формируемых датасетов. Для прикладной системы важно, чтобы данные были организованы не только по типу решаемой задачи технического зрения и формату данных, но и по смысловым группам, учитывающим сценарий применения, конфигурацию фона, условия наблюдения и пр.

Заключение

В работе представлен новый подход к реализации автоматизированного конвейера формирования больших наборов синтетических РЛИ X-диапазона, предназначенных для обучения системы группового технического зрения на базе многопозиционной РСА. Конвейер базируется на модифицированном симуляторе с растеризационным ядром и поддерживает генерацию сцен с различными типами подстилающей поверхности и классами наземных объектов. Реализована автоматическая аннотация данных для задач семантической сегментации и распознавания, а также механизмы масштабирования вычислений.

Промежуточные результаты подтверждают работоспособность подхода и повышение уровня реалистичности синтетических РЛИ для предобучения моделей. Производительность конвейера позволяет в приемлемые сроки формировать полноценные обучающие выборки.

Практическая значимость разработанных решений заключается в возможности ускоренного прототипирования нейросетевых моделей технического зрения для пространственно-распределенных бортовых радиолокационных систем без зависимости от дорогостоящих натурных экспериментов. Автоматизированный конвейер может быть интегрирован в процессы непрерывного обучения и дообучения моделей по мере поступления реальных данных, обеспечивая адаптацию системы к новым условиям эксплуатации.

Дальнейшее развитие конвейера будет направлено на повышение реалистичности формируемых синтетических РЛИ, обеспечение возможности генерации наборов разноразмерных данных и формирование оптимальной структуры датасетов для поддержания разнообразных сценариев при обучении и тестировании нейросетевых моделей.

Литература

1. Лялин К. С. Модульная многодиапазонная радиолокационная платформа дистанционного зондирования Земли с летательных аппаратов // Сб. докл. науч.-практ. спец. конф. в рамках Международного военно-технического форума (Кубинка, 16-18 авг. 2022). М: НПО "Специальная техника и связь" МВД РФ, 2022. С. 42-45.
2. Cha M., Majumdar A., Kung H.T., Barber J. Improving SAR Automatic Target Recognition Using Simulated Images Under Deep Residual Refinements // 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, 2018. pp. 2606-2610. DOI: 10.1109/ICASSP.2018.8462109.
3. Woollard M. et al. Synthetic aperture radar automatic target classification processing concept // Electronics Letters. 2019. Vol. 55. no. 24. pp. 1301-1303. DOI: 10.1049/el.2019.2389.
4. Тонких А.Н., Кузнецова В.А. Программный комплекс моделирования радиолокационных данных // Сборник научных статей по материалам VII Международной научно-практической конференции «Актуальные проблемы и перспективы развития радиотехнических и инфокоммуникационных систем» («Радиоинфоком-2023»). Москва: МИРЭА - Российский технологический университет, 2023. С. 43-46.
5. Ярцев И.М., Прохоров А.Г., Дмитриев И.Н. Технология создания системы нейросетевого автоматического распознавания одиночных наземных и надводных объектов вооружений, военной и специальной техники на основе системы исходных данных, полученных методом математического моделирования // Радиолокация: Теория и практика. Москва: ООО Издательство «Юнити-Дана», 2023. С. 299-315.
6. Balz T. Real-time SAR simulation on graphics processing units // Proceedings of the 6th European Conference on Synthetic Aperture Radar (EUSAR 2006). Dresden, Germany, 2006. <https://www.vde-verlag.de/proceedings-de/562960184.html>.

AUTOMATED SYNTHETIC RADAR IMAGES GENERATION IN THE DEVELOPMENT OF AIRCRAFT-BASED GROUP MACHINE VISION SYSTEM

leading researcher, PhD Kokutin S.N., engineer Sergiev S.A.

ANO HE «Innopolis University»

This article presents an approach to developing an automated pipeline for generating synthetic radar imagery sets to train neural network models used in aircraft-based group machine vision systems. The developed system is based on a modified simulator with a rasterization kernel that supports the input of 3D models of ground objects and raster masks representing various types of terrain surfaces. The simulator enhancement concept and the implemented pipeline architecture are described. Preliminary results demonstrate the feasibility of generating balanced datasets in volumes sufficient for large-scale training of neural network models. The proposed approach aims to address the scarcity of labeled real-world labeled radar images, which currently hinders the advancement of group machine vision technologies for aircraft-based radar systems



КЛАССИФИКАЦИЯ СЕТЕВЫХ АТАК В IIOT-СРЕДЕ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

доц. Лапина М.А., студ. Санамян О.А., студ. Семенов Г.А.

Северо-Кавказский федеральный университет,

Работа посвящена классификации сетевых атак в среде промышленного интернета вещей по признакам сетевого трафика. В качестве экспериментальной базы использован DataSense: CIC IoT Dataset 2025. Из исходного набора была сформирована выборка из 24087 записей, включающая 8 наиболее представленных типов атак. Перед обучением из данных исключались временные поля, соседние целевые метки, идентификаторы устройств и признаки, которые могли привести к утечке информации о классе. После очистки осталось 70 входных параметров. В эксперименте сравнивались Decision Tree, Random Forest, Linear SVM, Logistic Regression и Gaussian Naive Bayes. Модели оценивались по accuracy, macro precision, macro recall, macro F1-score, ROC-AUC, false positive rate и false negative rate. На выбранной выборке лучший weighted F1-score получен для Decision Tree. Random Forest показал близкое качество и наибольшее значение ROC-AUC, что делает его полезной альтернативой при анализе сетевых атак.

Введение

Промышленный интернет вещей применяется в системах, где сетевой обмен связан с работой датчиков, контроллеров и технологического оборудования [1]. В таких условиях атака на сеть может приводить не только к потере данных, но и к сбоям в рабочем процессе. Поэтому при анализе IIoT-трафика важно определять не только факт подозрительной активности, но и конкретный тип атаки.

В работе сравниваются классические алгоритмы машинного обучения для многоклассовой классификации атак по признакам сетевого трафика [2]. Такой подход выбран как базовый: он позволяет быстро получить воспроизводимые метрики, сравнить разные семейства моделей и отдельно рассмотреть характер ошибок с помощью матриц классификации, ROC-AUC, false positive rate и false negative rate.

1. Данные и методика эксперимента

Эксперимент выполнен на наборе DataSense: CIC IoT Dataset 2025 [3, 4]. Датасет подготовлен Canadian Institute for Cybersecurity и включает сетевые и сенсорные данные IIoT-среды, а также 50 типов атак, объединённых в 7 категорий [3, 4]. В качестве целевой переменной выбран столбец label3, где указан конкретный тип сетевой атаки.

Для эксперимента оставлены 8 наиболее представленных классов. Такая настройка позволила получить достаточно крупную подвыборку без сильного перекоса между редкими и массовыми атаками. Итоговый объём составил 24087 записей. Перед обучением из набора исключались временные поля, соседние целевые метки, идентификаторы устройств, IP/MAC-поля и длинные текстовые признаки. После этой очистки осталось 70 входных параметров. Обучающая и тестовая части формировались в пропорции 80/20 со стратификацией по классам.

В сравнении участвовали Decision Tree, Random Forest, Linear SVM, Logistic Regression и Gaussian Naive Bayes. Категориальные признаки кодировались методом one-hot encoding, числовые признаки нормализовались. Качество моделей оценивалось по accuracy, macro precision, macro recall, macro F1-score, ROC-AUC, false positive rate и false negative rate [5, 6].

2. Результаты эксперимента

Основные результаты сравнения моделей приведены в таблице 1. Лучшее значение weighted F1-score получила модель Decision Tree. Она достигла accuracy = 0,9653, macro F1-score = 0,9657 и false negative rate = 0,0332. Random Forest показал близкое качество и наибольшее значение ROC-AUC macro OVR, равное 0,9980. Gaussian Naive Bayes заметно уступил остальным моделям.

Таблица 1.

Сравнение качества моделей машинного обучения

Модель	Acc.	Prec.	Recall	F1	ROC-AUC	FPR	FNR
Decision Tree	0.9653	0.9652	0.9668	0.9657	0.9918	0.0050	0.0332
Random Forest	0.9604	0.9582	0.9604	0.9591	0.9980	0.0057	0.0396
Linear SVM	0.9317	0.9289	0.9351	0.9312	0.9963	0.0098	0.0649
Logistic	0.9232	0.9309	0.9260	0.9276	0.9958	0.0112	0.0740
Gaussian NB	0.8097	0.8667	0.8318	0.8040	0.9147	0.0278	0.1682

На рисунках 1 и 2 показано сравнение моделей по accuracy и macro F1-score. Значения первых четырёх моделей находятся в близком диапазоне, что указывает на хорошую разделяемость выбранных классов. Gaussian Naive Bayes имеет более низкие показатели, поэтому его можно рассматривать только как базовую вероятностную модель.

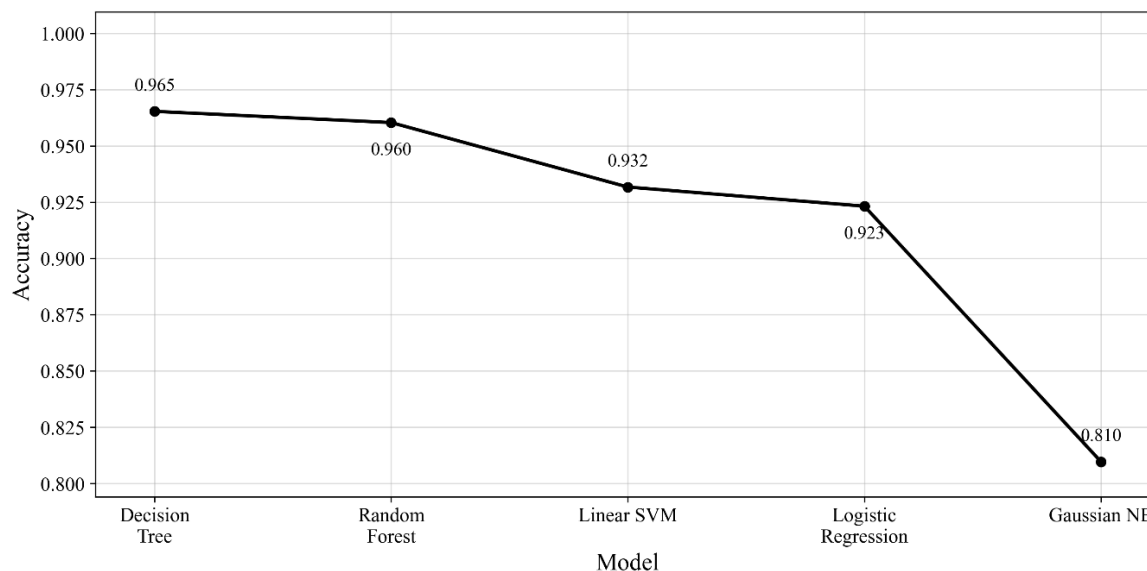


Рисунок 1. Сравнение моделей по accuracy

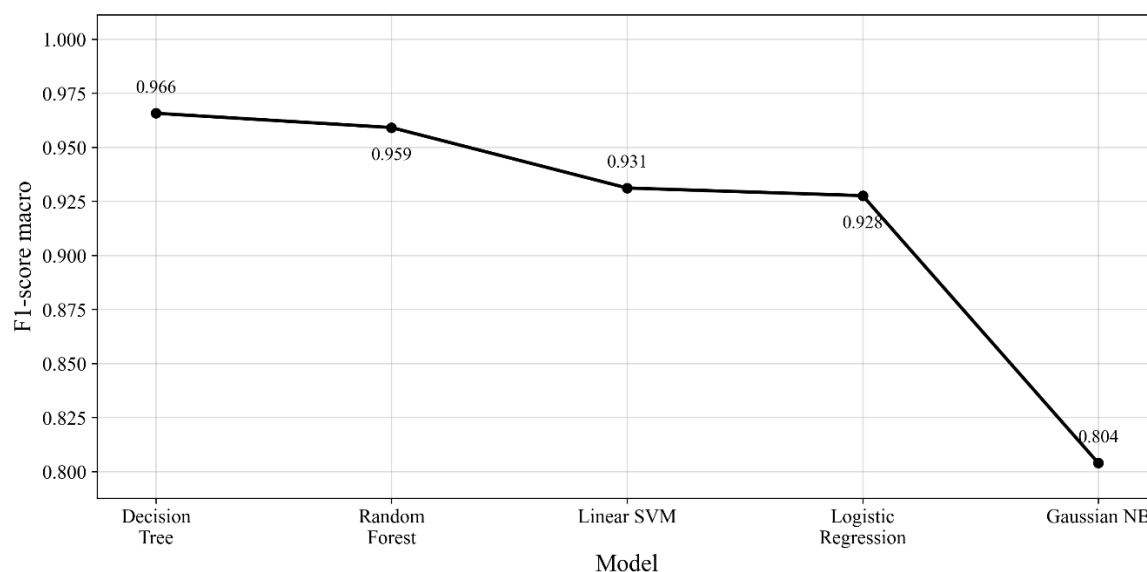


Рисунок 2. Сравнение моделей по macro F1-score

Для задач информационной безопасности особенно важна доля ложноотрицательных решений. На рисунке 3 видно, что Decision Tree имеет минимальный false negative rate, то есть реже остальных пропускает объекты своего класса. ROC-кривые на рисунке 4 дополнительно показывают, что Random Forest обладает наиболее высокой способностью к разделению классов.

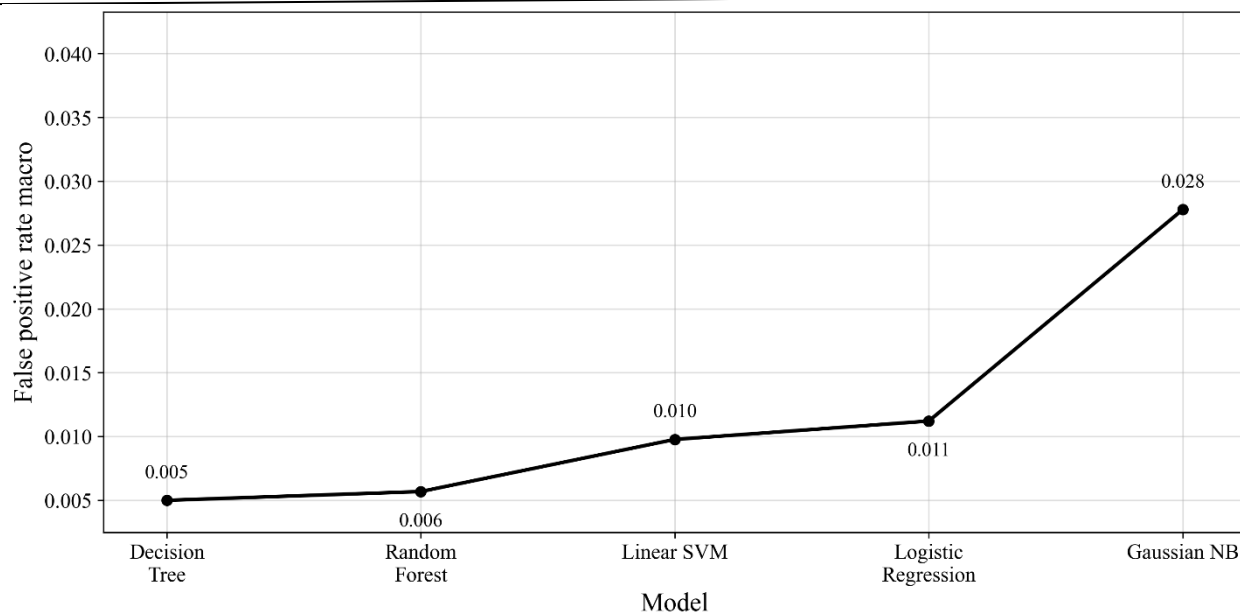


Рисунок 3. Сравнение моделей по macro false negative rate

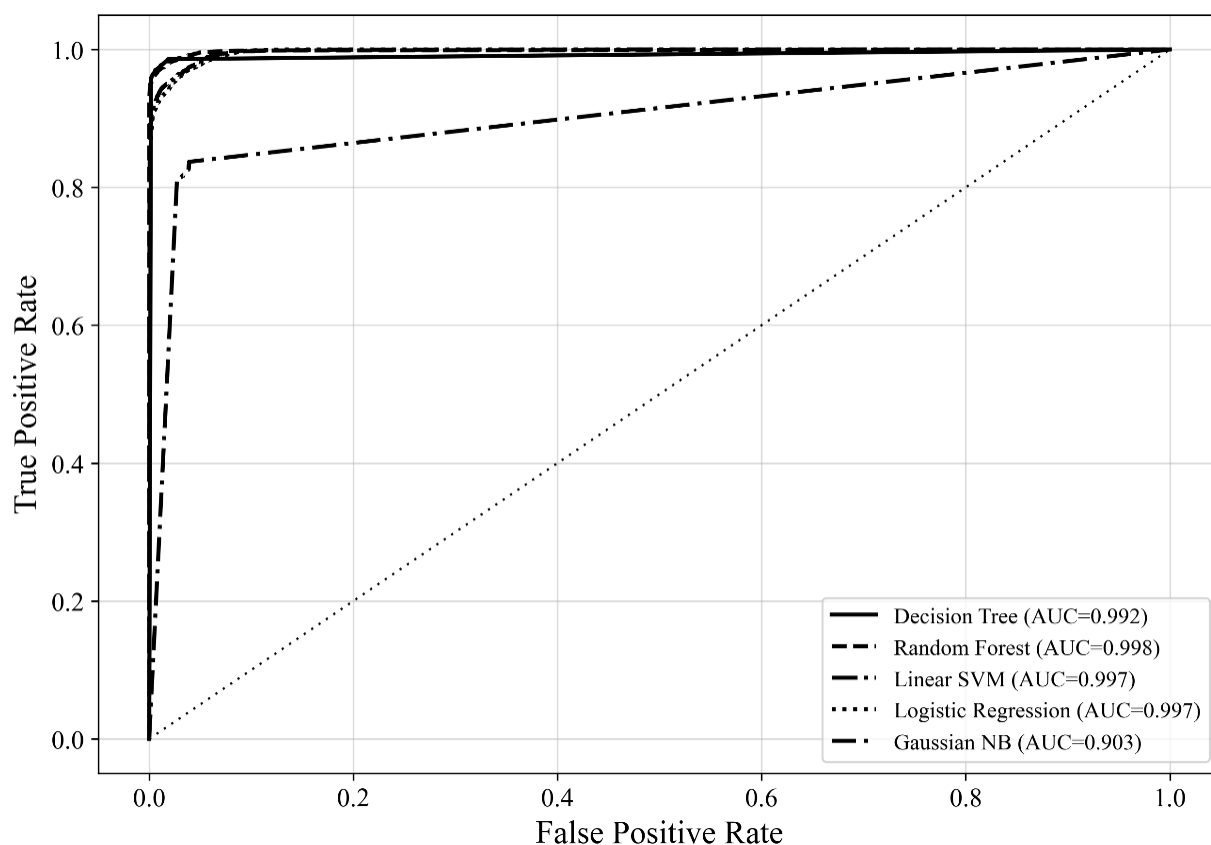


Рисунок 4. ROC-кривые для сравниваемых моделей

Нормализованная матрица ошибок Decision Tree представлена на рисунке 5. Основная часть значений расположена на главной диагонали. Ошибки в основном возникают между близкими типами flood-атак, что объясняется сходством их сетевых признаков.

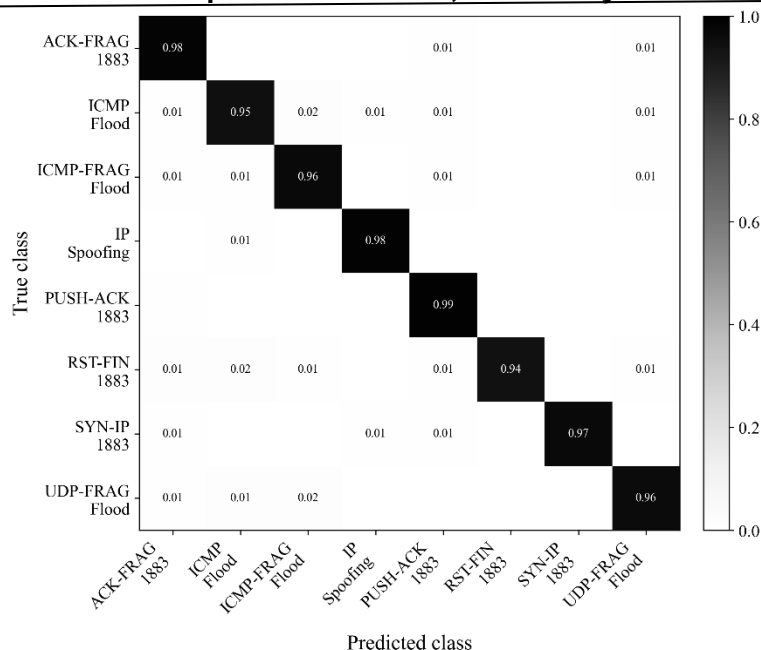


Рисунок 5. Нормализованная матрица ошибок Decision Tree

На рисунке 6 приведены наиболее значимые признаки Random Forest. Наибольший вклад внесли параметры, связанные с количеством портов, временными интервалами между пакетами, длиной IP-пакетов, размером полезной нагрузки, TCP-флагами и размером окна.

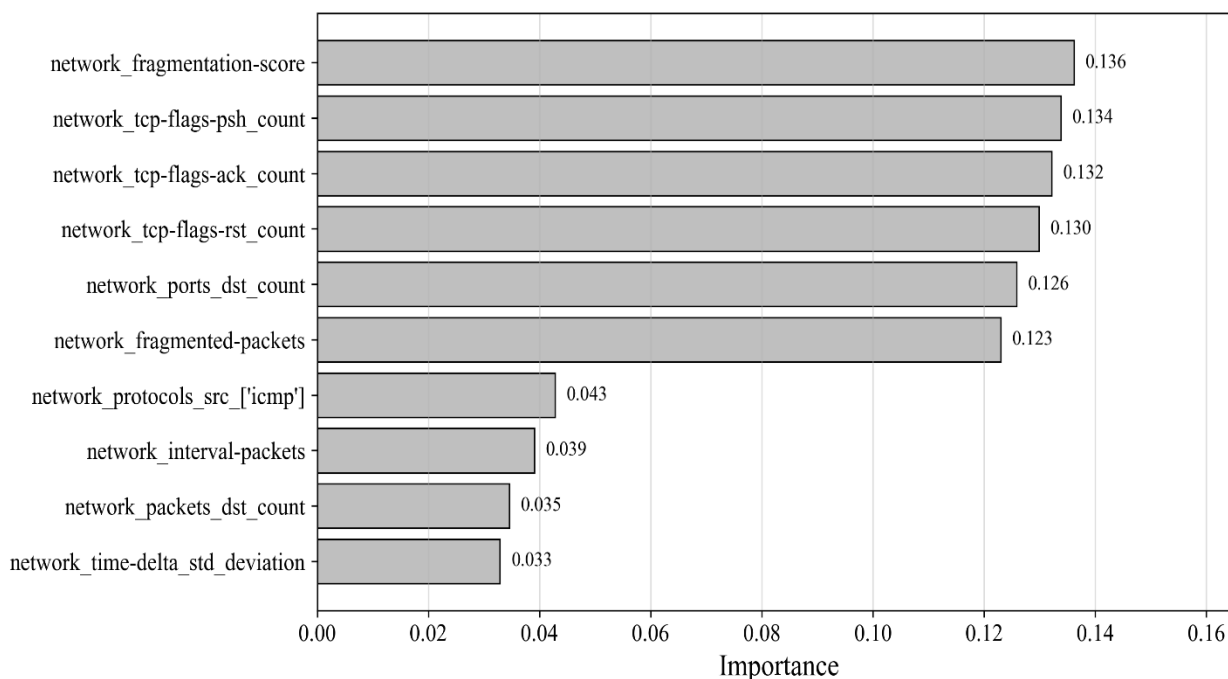


Рисунок 6. Наиболее значимые признаки Random Forest

Заключение

В работе сравнивались пять классических моделей машинного обучения для классификации атак в PoT-трафике. На выбранной подвыборке DataSense 2025 лучший итоговый результат получила Decision Tree: модель показала accuracy = 0,9653 и macro F1-score = 0,9657. Random Forest немного уступил по F1-score, но дал наибольшее значение ROC-AUC, поэтому его можно рассматривать как близкую по качеству альтернативу.

Матрица ошибок показала, что основные смещения возникают между близкими типами flood-атак. Это ожидаемо для сетевого трафика, где разные сценарии перегрузки могут иметь похожие признаки по длине пакетов, портам, временным интервалам и TCP-флагам. В дальнейшем эксперимент имеет смысл расширить за счёт большего числа классов и отдельной проверки редких атак.

Благодарности.

Исследование выполнено за счет гранта Российского научного фонда № 25-71-30007, <https://rscf.ru/project/25-71-30007/>.

Литература

1. Jawad M. A., Garcia J., Masoud M. A. A survey of Network Intrusion Detection Systems (NIDS) based on machine learning algorithms for Industrial Internet of Things (IIoT) // Conference on Sustainability and Cutting-Edge Business Technologies. — Cham : Springer Nature Switzerland, 2025. — P. 158–167.
2. Rusanov M., Babenko M., Lapina M., Sajid M. Identification of exploited unreliable account passwords in the information infrastructure using machine learning methods // Big Data and Cognitive Computing. — 2024. — Vol. 8, No. 11. — Article 159.
3. Firouzi A., Dadkhah S., Maret S. A., Ghorbani A. A. DataSense: A Real-Time Sensor-Based Benchmark Dataset for Attack Analysis in IIoT with Multi-Objective Feature Selection // Electronics. — 2025. — Vol. 14, No. 20. — Article 4095.
4. DataSense: CIC IIoT Dataset 2025 [Электронный ресурс] / Canadian Institute for Cybersecurity, University of New Brunswick. — URL: <https://www.unb.ca/cic/datasets/iiot-dataset-2025.html> (дата обращения: 13.05.2026).
5. SS K., MD D. S., S D. Internet of Things Network Intrusion Detection System Using Quantum and Classical Machine Learning // IET Quantum Communication. — 2025. — Vol. 6, No. 1. — Article e70020.
6. Pedregosa F., Varoquaux G., Gramfort A. et al. Scikit-learn: Machine Learning in Python // Journal of Machine Learning Research. — 2011. — Vol. 12. — P. 2825–2830.

CLASSIFICATION OF NETWORK ATTACKS IN IIOT ENVIRONMENT USING MACHINE LEARNING ALGORITHMS

assoc. prof. Lapina M.A., stud. Sanamyan O.A., stud. Semenov G.A.

North-Caucasus Federal University, Stavropol

The research addresses the classification of network attacks in an Industrial Internet of Things environment using network traffic features. The experimental part is based on DataSense: CIC IIoT Dataset 2025. A subset of 24087 records was formed from the original dataset and included 8 most represented attack types. Before model training, timestamp fields, auxiliary target labels, device identifiers and features that could cause data leakage were removed. After preprocessing, 70 input features remained. The experiment compared Decision Tree, Random Forest, Linear SVM, Logistic Regression and Gaussian Naive Bayes. Model quality was evaluated using accuracy, macro precision, macro recall, macro F1-score, ROC-AUC, false positive rate and false negative rate. On the selected subset, Decision Tree achieved the best weighted F1-score. Random Forest showed comparable classification quality and the highest ROC-AUC value, which makes it a useful alternative for network attack analysis.



ТЕРАГЕРЦОВАЯ ГРАФЕНОВАЯ ПЛАЗМОН-ПОЛЯРИТОННАЯ ФРАКТАЛЬНАЯ ПАТЧ-НАНОАНТЕННА С НЕЙРОСЕТЕВЫМ УПРАВЛЕНИЕМ

проф. Браже Р.А., магистрант Лебедев Е.Ю.

Ульяновский государственный технический университет

Благодаря высокой подвижности носителей заряда, двумерной структуре и возможности электрического управления параметрами графен рассматривается как перспективный материал для терагерцовых антенных систем [2,3]. В настоящей работе рассматривается терагерцовая графеновая плазмон-поляритонная фрактальная патч-наноантенна типа треугольного «ковра Серпинского», работающая в диапазоне 200–1300 ТГц. Особенность такой антенны состоит в том, что ее резонансные свойства определяются не только геометрией патча, но и дисперсией поверхностной проводимости графена, вследствие чего фрактализация начинает проявляться значительно сильнее, чем в гигагерцовом электромагнитном диапазоне [4-6]. В качестве основы используется планарная структура: графеновый патч расположен над диэлектрической подложкой и заземленной металлической пластиной, а возбуждение выполняется сигнальным проводником. Для практического использования многорезонансной антенны предложено нейросетевое управление режимом работы. Оно сводится к оценке качества принятого сигнала и выбору такой рабочей частоты, при которой приемно-передающий тракт обеспечивает требуемое качество связи. В качестве основной модели применяется одномерная сверточная сеть SignalPSNR, специально построенная для обработки сигналов без их преобразования в псевдоизображение. По результатам тестирования модель достигла точности 93,1%, что выше результатов ResNet18, VGG19 и U-Net.

Микрополосковые патч-антенны получили широкое распространение благодаря компактности, планарной структуре и простоте изготовления [1]. Для гигагерцового диапазона показано, что фрактализация не увеличивает число рабочих частот и не расширяет полосу пропускания, а чаще всего лишь смещает резонансы и усложняет конструкцию. Однако данный вывод нельзя переносить на терагерцовый диапазон, где физическая природа процессов в проводящем слое изменяется [6].

При переходе к терагерцовым частотам и нанометровым размерам в графеновом патче возбуждаются поверхностные плазмон-поляритоны. Они представляют собой связанные колебания электромагнитного поля и электронной плотности. В отличие от обычных электромагнитных волн, такие колебания обладают сильной дисперсией, поэтому их фазовая скорость и эффективная длина волны зависят от частоты, химического потенциала графена, параметров подложки и затворного напряжения. Именно это делает фрактальную геометрию в графеновых наноантеннах не просто усложнением геометрии, а способом формирования набора рабочих резонансов [6].

На рисунке 1 приведена геометрия исследуемой фрактальной патч-наноантенны. В качестве исходной формы используется треугольник Серпинского в 0, 1, 2 и 3 итерациях. Для терагерцовой реализации материалом патча является графен; диэлектрическая подложка выполнена из карбида кремния SiC с относительной диэлектрической проницаемостью $\epsilon_r = 9,66$. Длина стороны большого треугольника равна $s = 625$ нм, толщина подложки $t = 10$ нм, ширина сигнального проводника $W = 40$ нм.

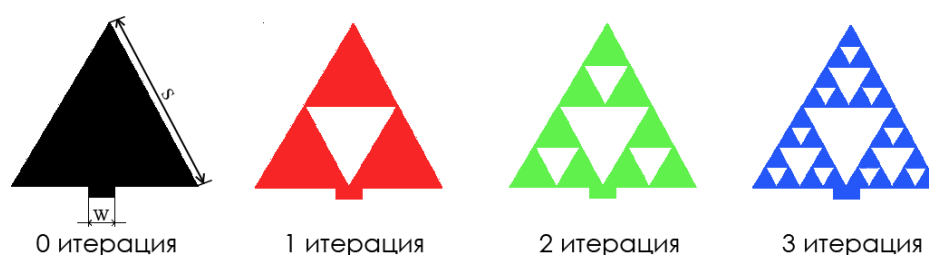


Рисунок 1. Геометрия фрактальной патч-наноантенны: для ТГц-антенны материал – графен, $s = 625$ нм; диэлектрик – SiC ($\epsilon_r = 9,66$), $t = 10$ нм; $W = 40$ нм

Между графеновым патчем и заземленной металлической пластиной находится диэлектрик. При приложении затворного напряжения положительной полярности уровень Ферми в графене смещается относительно точки Дирака, что позволяет реализовать электронную проводимость и управлять плазмон-поляритонными свойствами структуры. Для расчета характеристик такой антенны в модели применяется частотная зависимость поверхностной проводимости графена. В первом приближении она описывается моделью Друде [6].

Математическое моделирование выполняется в CST Microwave Studio. В отличие от гигагерцовой патч-антенны, где фрактализация в основном не меняет количество резонансов, графеновая плазмон-поляритонная наноантенна демонстрирует выраженную многополосность. Для нулевой итерации в диапазоне 200–1300 ТГц наблюдается один основной резонанс около 238 ТГц. Уже первая итерация дает

набор рабочих частот 246, 371, 517, 657 и 776 ТГц. Для второй итерации характерны резонансы около 233, 437, 664, 859 и 1075 ТГц, а для третьей – около 213, 343, 673, 972 и 1294 ТГц.

В большинстве режимов коэффициент стоячей волны по напряжению находится вблизи диапазона 1,1–2,0, а входной импеданс остается в интервале, удобном для дальнейшего согласования с приемно-передающим устройством. Это означает, что фрактальная графеновая наноантенна может рассматриваться не как один фиксированный излучатель, а как набор допустимых частотных режимов, между которыми можно переключаться.

Однако само наличие нескольких резонансов еще не решает задачу устойчивой связи. Качество приема определяется не только антенной, но и передатчиком, каналом распространения, уровнем шума, помехами и алгоритмами цифровой обработки. Поэтому управление характеристиками в данной работе понимается не как механическое изменение формы патча, а как интеллектуальный выбор режима, соответствующего одному из резонансов антенны. Если на текущей частоте сигнал становится недостаточно качественным, передатчик и приемник должны быть согласованно переведены на другую рабочую частоту.

Для решения этой задачи используется нейросетевая оценка качества сигнала. На вход модели подается окно из 1024 нормированных отсчетов принятого сигнала. Выходом является вероятность принадлежности текущего окна к классу качественного или некачественного сигнала. Если вероятность качественного приема выше заданного порога, система сохраняет текущую рабочую частоту. Если же вероятность оказывается ниже порога, контроллер инициирует переход на другой резонансный режим антенны и повторяет оценку для нового частотного канала.

Ключевым элементом такого контура является модель SignalPSNR. В отличие от ResNet18, VGG19 и U-Net, которые в рассматриваемой задаче требуют преобразования одномерного сигнала в двумерное представление, SignalPSNR обрабатывает временную последовательность непосредственно [7-9]. Архитектура включает начальный одномерный сверточный блок, несколько остаточных блоков ResidualBlock1D, механизмы Squeeze and Excitation, TemporalAttention, глобальное усреднение, а также полносвязный классификатор [10]. Такая структура позволяет выделять как локальные искажения формы сигнала, так и устойчивые признаки качества во всем временном окне.

На рисунке 2 приведены точности обучения и тестирования для четырех моделей. ResNet18 быстро выходит на уровень около 81–82% на тестовой выборке, но при дальнейшем росте обучающей точности демонстрирует признаки переобучения. VGG19 обучается более ровно, однако ее итоговая точность ниже. U-Net показывает лучший результат среди сравниваемых архитектур, но уступает специализированной одномерной модели. Максимальная точность SignalPSNR на тестовой выборке составила 93,1%, тогда как для U-Net она равна 83,5%, для ResNet18 – 81,6%, а для VGG19 – 73,1%.

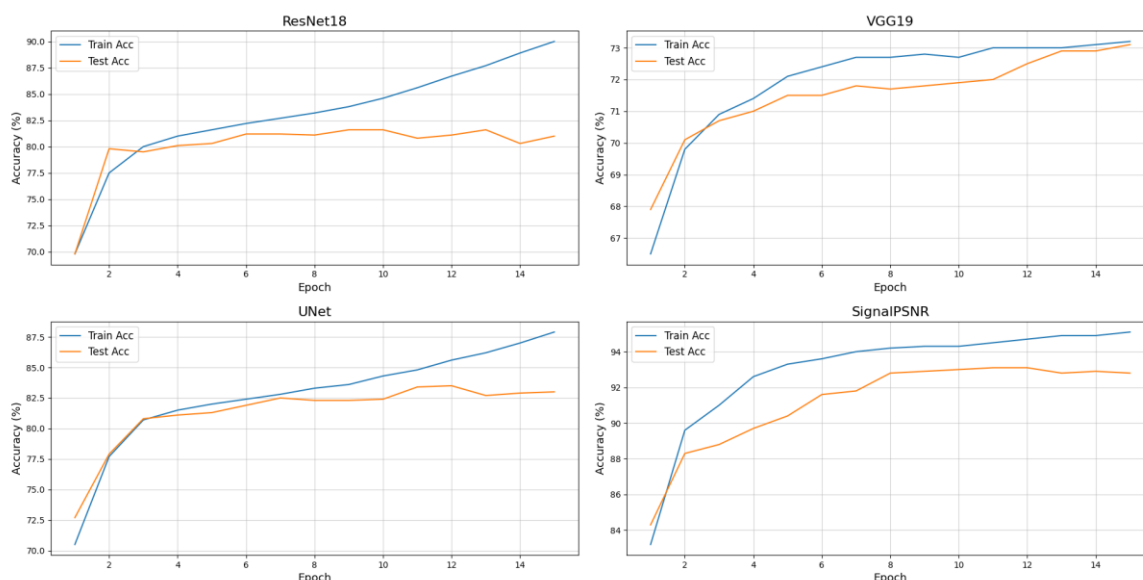


Рисунок 2. Графики зависимости точности обучения и тестирования от номера эпохи для моделей ResNet18, VGG19, U-Net и SignalPSNR

Использование нейросетевого управления позволяет связать многорезонансность антенны с текущим состоянием канала. В простейшем варианте алгоритм можно представить следующим образом: приемник формирует окно сигнала, выполняется нормализация, модель SignalPSNR вычисляет вероятность качественного приема, после чего контроллер либо сохраняет текущий режим, либо переводит тракт на другую разрешенную частоту. При наличии нескольких допустимых резонансов переход может

осуществляться не вслепую, а с учетом ранее накопленной статистики качества, доступной полосы, допустимой задержки и требований к энергетической эффективности.

Такой подход принципиально отличается от традиционного подбора антенны под одну фиксированную частоту. Сама антенна остается планарной и не требует механической перестройки. Управляющее воздействие переносится на уровень выбора режима передатчика и приемника, что особенно важно для миниатюрных терагерцевых систем связи, где любые механические или сложные коммутационные элементы нежелательны.

Следовательно, фрактализация в терагерцевом диапазоне частот выполняет две функции. Во-первых, она увеличивает число наблюдаемых рабочих резонансов за счет взаимодействия плазмон-поляритонных мод с элементами разных масштабов [6].

Во-вторых, она создает набор частотных состояний, которыми можно управлять алгоритмически. Нейросеть, в свою очередь, не моделирует антенну заново, а оценивает результат ее работы в составе реального тракта и тем самым замыкает контур адаптивного управления.

Формально множество допустимых частот можно записать как $F = (f_1, f_2, \dots, f_n)$, где каждая частота соответствует одному из устойчивых резонансных состояний наноантенны. Для каждого состояния приемник получает фрагмент сигнала x , а нейросетевая модель вычисляет величину $q = P(\text{качество} | x)$. Если q превышает установленное пороговое значение, данный частотный режим считается пригодным для дальнейшей передачи. Если q мало, система либо переходит к следующей частоте из множества F , либо выбирает частоту с наибольшим ожидаемым значением q , если такая статистика уже накоплена в памяти контроллера.

Подобная схема удобна тем, что она не требует заранее описывать все возможные виды искажений. Простое сравнение мощности сигнала может быть недостаточным, поскольку мощный сигнал не всегда является пригодным для корректного восстановления информации. Нейросеть же оценивает целое временное окно и способна учитывать форму сигнала, локальные выбросы, шумовую составляющую и устойчивость полезной структуры.

Важным преимуществом SignalPSNR является работа в режиме реального времени. После обучения модель выполняет только прямой проход по сети, состоящий из сверточных операций, операций нормализации, функций активации и нескольких полносвязных преобразований. Задержка принятия решения может быть сделана меньше характерного времени изменения условий канала.

В то же время предлагаемая схема не отменяет необходимости согласования. Для каждого выбранного резонанса необходимо обеспечить приемлемый КСВН, входной импеданс, устойчивую диаграмму направленности и достаточный уровень излучения. Нейросетевой алгоритм не способен исправить заведомо непригодный аппаратный режим, но он может выбрать лучший из допустимых. Поэтому проектирование такой системы должно рассматриваться как совместная задача моделирования, схемотехнического согласования и обучения модели оценки качества сигнала.

Сочетание графеновой плазмон-поляритонной фрактальной патч-наноантенны и нейросетевых моделей является перспективным направлением для терагерцевых систем связи. В отличие от гигагерцевых фрактальных патчей, где усложнение формы часто не дает выигрыша, в графеновых терагерцевых структурах фрактальность проявляется через дисперсию и приводит к появлению нескольких рабочих резонансов. Нейросетевая модель SignalPSNR позволяет сохранять текущую частоту при хорошем качестве сигнала и переходить на другой режим при ухудшении приема.

Литература

1. Al-Zabee A.A.K., Jabbar S.Q., Wang D. Fractal antennas (Study and Review) // International Journal of Computers and Technology. – 2016. – Vol. 15, № 13. – P. 7387–7400.
2. Boretti A., Rosa L., Blackledge J., Castelletto S. A preliminary study of a graphene fractal Sierpinski antenna // IOP Conference Series: Materials Science and Engineering. – 2020. – Vol. 840. – P. 012003.
3. Blackledge J., Boretti A., Rosa L., Castelletto S. Fractal graphene patch antennas and the THz communications revolution // IOP Conference Series: Materials Science and Engineering. – 2021. – Vol. 1060. – P. 012001.
4. Rosa L., Sun K., Juodkazis S. Sierpinski fractal plasmonic nanoantennas // Physica Status Solidi RRL. – 2011. – Vol. 5, № 5–6. – P. 175–177.
5. Sederberg S., Elezzabi A.Y. Sierpinski fractal plasmonic antenna: A fractal abstraction of the plasmonic bowtie antenna // Optics Express. – 2011. – Vol. 19, № 11. – P. 10456–10461.
6. Браже Р.А., Лебедев Е.Ю. Фрактальная графеновая плазмон-поляритонная патч-наноантенна для ближнего инфракрасного и оптического диапазонов частот // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2024. – № 2. – С. 98–111.
7. He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. – 2016. – P. 770–778.

8. Simonyan K., Zisserman A. Very deep convolutional networks for large-scale image recognition // International Conference on Learning Representations. – 2015.
9. Ronneberger O., Fischer P., Brox T. U-Net: Convolutional networks for biomedical image segmentation // Medical Image Computing and Computer-Assisted Intervention. – 2015. – P. 234–241.
10. Hu J., Shen L., Sun G. Squeeze-and-Excitation Networks // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. – 2018. – P. 7132–7141.

TERAHERTZ GRAPHENE PLASMON-POLARITON FRACTAL PATCH NANOANTENNA WITH NEURAL NETWORK CONTROL

Prof. Brazhe R.A., Master's degree stud. Lebedev E.Yu.

Ulyanovsk State Technical University

Due to the high mobility of charge carriers, two-dimensional structure and the possibility of electrical parameter control, graphene is considered as a promising material for terahertz antenna systems. In this paper, we consider a terahertz graphene plasmon-polariton fractal patch nanoantenna of the Sierpinski triangular carpet type operating in the range of 200-1300 THz. The peculiarity of such antenna is that its resonant properties are determined not only by the geometry of the patch, but also by the dispersion of the surface conductivity of graphene, as a result of which fractalization begins to manifest itself much more strongly than in the gigahertz electromagnetic range. A planar structure is used as the basis: a graphene patch is located above a dielectric substrate and a grounded metal plate, and the excitation is performed by a signal conductor. For practical use of a multiresonance antenna, neural network mode control is proposed. It boils down to evaluating the quality of the received signal and selecting an operating frequency at which the receiving and transmitting path provides the required communication quality. The one-dimensional convolutional network SignalPSNR is used as the main model, which is specially built for signal processing without converting them into a pseudo-image. According to the test results, the model achieved an accuracy of 93.1%, which is higher than the results of ResNet18, VGG19 and U-Net.



ВЫБОР СТРУКТУРЫ НЕЙРОННОЙ СЕТИ ДЛЯ РАСПОЗНАВАНИЯ ПОЖАРОВ ПО ОПТИЧЕСКИМ ИЗОБРАЖЕНИЯМ

студ. Марченков М.О.

Московский технический университет связи и информатики

В работе рассматриваются методы обнаружения пожаров на изображениях с использованием беспилотных летательных аппаратов и сверточных нейронных сетей. Проведен сравнительный анализ моделей YOLOv5, YOLOv8 и Faster R-CNN с точки зрения их применимости для бортовых систем.

Сформирован собственный датасет изображений пожаров, на основе которого выполнено обучение и тестирование моделей. Разработана кастомизированная модель на базе YOLOv5, адаптированная под задачу детекции пожаров.

Показано, что облегченные нейросетевые архитектуры обеспечивают необходимое качество детекции при ограниченных вычислительных ресурсах, что позволяет применять их в системах бортовой обработки данных БПЛА.

Введение

В последние годы задача своевременного обнаружения пожаров становится особенно актуальной в связи с увеличением числа возгораний природного и техногенного характера. Эффективность мониторинга напрямую зависит от скорости выявления очагов, что требует применения современных технических решений. Одним из таких решений является использование беспилотных летательных аппаратов, позволяющих получать изображения высокого разрешения в режиме реального времени [1].

Однако применение БПЛА сопровождается рядом ограничений, связанных с необходимостью обработки значительных объемов визуальной информации при ограниченных вычислительных ресурсах бортовых систем. Передача данных на наземные станции увеличивает задержки и предъявляет высокие требования к каналам связи, что снижает оперативность реагирования [2, 3]. В связи с этим актуальной задачей является разработка алгоритмов, способных выполнять обработку изображений непосредственно на борту БПЛА.

Современные методы анализа изображений преимущественно основаны на применении нейронных сетей [4, 5]. Наибольшее распространение получили сверточные нейронные сети, которые позволяют автоматически выделять информативные признаки и эффективно решать задачи компьютерного зрения [6-8]. Развитие данных подходов привело к появлению специализированных архитектур для детекции объектов, позволяющих одновременно определять наличие объектов и их пространственное положение на изображении. К наиболее распространенным относятся модели семейства YOLO, а также двухэтапные алгоритмы, такие как Faster R-CNN [16, 17]. Архитектура модели YOLO представлена на рисунке 1 и подробно рассмотрена в работе [16].

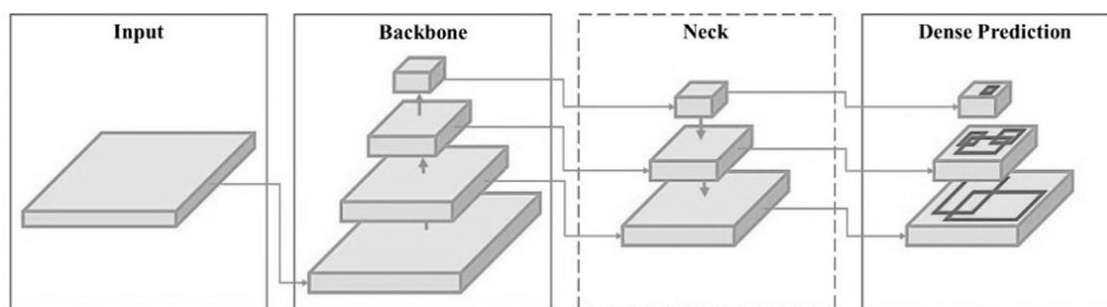


Рисунок 1 – Архитектура модели Yolo

Несмотря на высокие показатели точности, многие существующие модели характеризуются значительной вычислительной сложностью, что ограничивает их применение в бортовых системах. В связи с этим особую актуальность приобретает задача выбора и адаптации нейросетевых архитектур, обеспечивающих оптимальное соотношение точности и вычислительной эффективности. Кроме того, важным аспектом является формирование специализированных обучающих выборок, учитывающих особенности обнаружения пожаров, включая различный масштаб очагов возгорания и условия съемки [15].

Таким образом, в рамках данной работы рассматривается задача разработки бортового алгоритма распознавания изображений для обнаружения пожаров с использованием методов глубокого обучения. Особое внимание уделяется анализу существующих архитектур нейронных сетей, формированию

обучающего датасета, а также разработке и оптимизации модели, пригодной для использования в условиях ограниченных вычислительных ресурсов.

Разработка и исследование бортового алгоритма распознавания изображений

Качество работы нейросетевых моделей во многом определяется характеристиками обучающей выборки. В рамках данной работы был сформирован собственный датасет, включающий около 4000 изображений, содержащих сцены с различными типами пожаров. Подобные подходы к формированию обучающих выборок широко применяются в задачах мониторинга с использованием БПЛА [11, 12].

При формировании датасета учитывалось разнообразие входных данных, включая различия в масштабе очагов возгорания. Выборка включает крупные, средние и малые пожары, при этом основной акцент сделан на средние и малые объекты как наиболее сложные для обнаружения. Такой подход позволяет повысить обобщающую способность модели и улучшить качество детекции.



Рисунок 2 – Примеры изображений из созданного обучающего датасета с пожаром и без пожара

Для повышения устойчивости модели к изменениям входных данных обучающая выборка была дополнена изображениями, полученными в различных условиях съемки, включая вариации освещенности, погодных факторов и высоты наблюдения. Кроме того, применялись методы аугментации изображений, направленные на увеличение объема выборки и улучшение качества обучения модели [9, 10].

Далее было выполнено экспериментальное сравнение различных архитектур нейронных сетей, применяемых для решения задачи детекции объектов. В качестве основных моделей были выбраны YOLOv5n, YOLOv8n и Faster R-CNN, что обусловлено их широким применением в области компьютерного зрения [16-20].

Обучение всех моделей проводилось на одном и том же датасете с использованием одинаковых параметров, что позволило обеспечить сопоставимость результатов. Полученные значения метрик качества представлены в таблице 1.

Главным параметром, определяющим качество детекции, является mAP (mean Average Precision) – показывающий среднюю точность обнаружения объектов при пороге перекрытия IoU (Intersection over Union) равном 0.5. Формула приведена ниже [10, 14]:

$$mAP50 = \frac{1}{N} \sum_{i=1}^N AP_i$$

где:

N – количество классов (в моём случае N=1, так как класс "fire").

AP_i – средняя точность.

Таблица 1

Результаты сравнения моделей

Модель	mAP50	mAP50-95	Вывод
Yolo v5n	0.859	0.504	Лучшая
Yolo v8n	0.832	0.52	Средняя
Faster R-CNN	0.761	0.429	Медленная

Результаты экспериментов показали, что модель Faster R-CNN, несмотря на высокую точность локализации объектов, характеризуется значительной вычислительной сложностью и низкой скоростью обработки изображений. Это делает её малоприменимой для использования на борту БПЛА, где критическим фактором является возможность работы в режиме реального времени. Модель YOLOv8n продемонстрировала более высокую скорость работы, однако по совокупности показателей не обеспечила существенного преимущества.

По результатам проведенного анализа модель YOLOv5n продемонстрировала наилучшее соотношение точности и скорости обработки. Значения метрик составили $mAP50 = 0.859$ и $mAP50-95 = 0.504$, что свидетельствует о высокой эффективности детекции при сохранении производительности. Это позволило использовать данную архитектуру в качестве базовой для дальнейшей разработки алгоритма.

Для адаптации модели к специфике задачи обнаружения пожаров была реализована её модификация, включающая настройку параметров обучения и упрощение архитектуры под один класс объектов. Это позволило повысить применимость модели к специализированному датасету и улучшить стабильность работы при различных условиях.

Результаты работы кастомизированной модели показали сопоставимый уровень точности по сравнению с базовой версией. Результаты показаны в таблице 2.

Таблица 2

Результаты кастомизированной модели Yolo v5n

Метрика	Значение
Precision	0.817
Recall	0.777
mAP50	0.838
mAP50-95	0.431

Для дополнительного повышения точности была рассмотрена более сложная архитектура YOLOv5m. Увеличение разрешения входных данных и числа эпох обучения позволило улучшить показатели детекции, однако сопровождалось ростом вычислительной нагрузки, что ограничивает применение модели в бортовых системах.

Полученные результаты показали, что использование более сложной модели действительно позволяет повысить показатели точности и полноты детекции. Однако данный подход сопровождается существенным увеличением вычислительных затрат и энергопотребления, что является критическим ограничением при использовании модели на борту БПЛА.

Таким образом, проведенный анализ показал, что увеличение сложности нейронной сети не всегда является оправданным, особенно в условиях ограниченных ресурсов. Несмотря на более высокие показатели качества, модель YOLOv5m не может быть эффективно использована в бортовых системах без дополнительной оптимизации.

В результате в качестве оптимального решения была выбрана кастомизированная модель на базе YOLOv5n, обеспечивающая баланс между точностью детекции, вычислительной эффективностью и устойчивостью работы на специализированном датасете.

Таким образом, в рамках данной главы была реализована и исследована модель обнаружения пожаров, адаптированная для использования в условиях ограниченных вычислительных ресурсов. Полученные результаты подтверждают возможность создания эффективных бортовых алгоритмов распознавания изображений, обеспечивающих высокую точность и скорость работы при минимальных затратах ресурсов.

Вывод

В работе проведен анализ методов детекции пожаров на основе сверточных нейронных сетей и выполнено сравнение моделей YOLOv5n, YOLOv8n и Faster R-CNN. Установлено, что наилучшее соотношение точности и скорости демонстрирует модель YOLOv5n ($mAP50 = 0.859$, $mAP50-95 = 0.504$), что делает её наиболее подходящей для бортового применения.

На основе выбранной архитектуры разработана кастомизированная модель, показавшая сопоставимые показатели точности ($mAP50 = 0.838$) по сравнению с базовой версией ($mAP50 = 0.859$), при этом ориентированная на работу в условиях ограниченных ресурсов и специализированного датасета.

Таким образом, установлено, что увеличение сложности модели повышает точность, но ограничивает её применение на борту БПЛА. Оптимальным решением является кастомизированная модель YOLOv5n,

Литература

1. Чиров Д.С., Марченков М.О. Анализ алгоритмов распознавания пожаров на изображениях, полученных оптико-электронной системой БПЛА // Системы синхронизации, формирования и обработки сигналов. 2025. Т. 16. № 6. С. 23-26. EDN: WXTLSW.
2. Чиров Д.С., Иванкович М.В., Гололобов И.Л. Построение каналов связи с БПЛА среднего и дальнего радиуса действия // Электросвязь. 2025. № 4. С. 47-52. DOI: 10.34832/ELSV.2025.66.4.006.
3. Чиров Д.С., Лобов Е.М. Выбор сигнально-кодовой конструкции для командно-телеметрической линии радиосвязи с беспилотными летательными аппаратами средней и большой дальности // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11. № 10. С. 21-28. EDN: ZTBQEI.
4. Виноградов А.Н., Макаренков С.А., Чиров Д.С. Применение методов Data Mining для формирования базы знаний экспертной системы классификации радиосигналов // T-Comm: Телекоммуникации и транспорт. 2010. Т. 4. № 11. С. 61-64. EDN: OKEWBX.
5. Чиров Д.С., Стецюк А.Н. Применение искусственных нейронных сетей в бортовых системах специальных робототехнических комплексов // Нейрокомпьютеры: разработка, применение. 2017. № 3. С. 42-43. EDN: YZIRAZ.
6. Гонсалес Р., Вудс Р. Цифровая обработка изображений. – М.: Техносфера, 2012. – 1104 с.
7. Сойфер В.А. Методы компьютерного зрения. – М.: Физматлит, 2008. – 784 с.
8. Кудрявцев А.А., Кузнецов В.В. Нейронные сети и глубокое обучение. – СПб.: Питер, 2019. – 480 с.
9. Баранов А.В., Смирнов С.В. Применение нейронных сетей для обработки изображений в системах мониторинга // Информационные технологии. – 2021. – №5. – С. 23–30.
10. Иванов Д.А., Петров И.С. Методы обнаружения объектов на изображениях с использованием глубокого обучения // Вестник МГТУ им. Н.Э. Баумана. – 2020. – №4. – С. 45–56.
11. Козлов А.Н. Беспилотные летательные аппараты: основы, системы и применение. – М.: Машиностроение, 2018. – 320 с.
12. Сидоров В.П., Орлов Н.Г. Анализ методов обнаружения пожаров с использованием БПЛА // Современные проблемы науки и образования. – 2022. – №2.
13. Захаров Е.В. Применение методов компьютерного зрения в системах мониторинга окружающей среды // Автоматизация и управление. – 2021. – №6. – С. 12–19.
14. Попов И.А., Лебедев К.С. Использование сверточных нейронных сетей для анализа изображений // Научно-технический вестник ИТМО. – 2020. – №3. – С. 78–85.
15. Морозов А.Д. Обработка изображений в реальном времени в встраиваемых системах // Электроника и вычислительная техника. – 2019. – №8. – С. 34–41.
16. Redmon J., Divvala S., Girshick R., Farhadi A. You Only Look Once: Unified, Real-Time Object Detection // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). – 2016.
17. Ren S., He K., Girshick R., Sun J. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 2017.
18. Goodfellow I., Bengio Y., Courville A. Deep Learning. – Cambridge: MIT Press, 2016.
19. Jocher G. et al. YOLOv5 // GitHub repository. – URL: <https://github.com/ultralytics/yolov5> (дата обращения: 10.04.2026).
20. Ultralytics. YOLOv8 Documentation. – URL: <https://docs.ultralytics.com> (дата обращения: 10.04.2026).

SELECTION OF A NEURAL NETWORK STRUCTURE FOR FIRE RECOGNITION FROM POTIC IMAGES

student Marchenkov M.O.

Moscow Technical University of Communications and Informatics

This paper examines methods for detecting fires in images using unmanned aerial vehicles (UAVs) and convolutional neural networks. A comparative analysis of the YOLOv5, YOLOv8, and Faster R-CNN models is conducted for their applicability to onboard systems.

A proprietary dataset of fire images was created, which was used to train and test the models. A customized model based on YOLOv5, adapted for fire detection, was developed.

It is shown that lightweight neural network architectures provide the required detection quality with limited computing resources, making them suitable for use in onboard UAV data processing systems.



СЛАБЫЕ ПАРОЛИ КАК ФАКТОР КОМПРОМЕТАЦИИ УЧЕТНЫХ ЗАПИСЕЙ: СОВРЕМЕННЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ И АНАЛИЗА

асп. Русанов М.А.¹, доц. Лапина М.А.²

¹Московский финансово-юридический университет,

²Северо-Кавказский федеральный университет.

В работе представлен обзор современных методов выявления слабых паролей в информационных системах организаций. Рассмотрены основные причины использования ненадежных паролей, включая человеческий фактор, ограничения традиционных парольных политик, повторное использование учетных данных и наличие локальных учетных записей. Проведен анализ существующих подходов к обнаружению слабых паролей, основанных на словарных атаках, статистических моделях, методах password guessing и алгоритмах машинного обучения. Особое внимание уделено проблеме дефолтных и локальных паролей, не подпадающих под действие централизованных политик безопасности. Рассмотрены современные методы оценки стойкости парольной информации и подходы к повышению эффективности защиты учетных записей. Сделан вывод о перспективности применения интеллектуальных методов анализа и машинного обучения для автоматизированного выявления уязвимых паролей в корпоративной инфраструктуре.

Ключевые слова: информационная безопасность, слабые пароли, password guessing, password auditing, машинное обучение, парольная политика, локальные учетные записи, дефолтные пароли, оценка стойкости паролей.

Введение

В современных условиях развития информационных технологий парольная аутентификация продолжает оставаться одним из наиболее распространенных механизмов контроля доступа к информационным ресурсам. Несмотря на активное внедрение многофакторной аутентификации, биометрических методов идентификации и аппаратных средств защиты, пароли сохраняют ключевую роль в обеспечении безопасности корпоративных информационных систем. Однако эффективность парольной защиты непосредственно зависит от качества создаваемых пользователями паролей и корректности их использования.

Практика эксплуатации информационных систем показывает, что значительная часть пользователей использует слабые, предсказуемые или повторно применяемые пароли. Дополнительную проблему представляет тот факт, что многие пароли формально удовлетворяют требованиям парольной политики, но при этом остаются уязвимыми для современных методов подбора. Существенные риски также связаны с локальными учетными записями и системными учетными данными, на которые корпоративные политики безопасности зачастую не распространяются.

Злоумышленники активно применяют автоматизированные средства password guessing, словарные атаки, статистические модели и алгоритмы машинного обучения для компрометации учетных записей пользователей. В связи с этим задача своевременного выявления слабых паролей становится одним из важнейших направлений обеспечения информационной безопасности организации.

Целью работы является обзор современных методов обнаружения слабых паролей, анализ существующих подходов к оценке стойкости парольной информации, а также исследование методов выявления локальных, системных и формально корректных, но уязвимых паролей.

1. Причины появления слабых паролей

Одной из основных причин распространения слабых паролей является человеческий фактор. Пользователи стремятся создавать пароли, которые легко запомнить и воспроизвести, вследствие чего широко применяются общеизвестные слова, имена, даты, а также простые последовательности символов.

В работе [1] отмечается, что чрезмерно строгие требования парольных политик нередко приводят к обратному эффекту. Пользователи начинают использовать предсказуемые способы модификации паролей, включая замену отдельных букв цифрами, добавление специальных символов в конец строки или использование типовых шаблонов. В результате пароль формально соответствует требованиям политики безопасности, однако остается уязвимым для современных методов анализа и подбора.

Авторы исследования подчеркивают, что проблема заключается не только в недостаточной сложности пароля, но и в предсказуемости поведения пользователей. Стремление минимизировать когнитивную нагрузку приводит к формированию повторяющихся шаблонов, которые могут эффективно использоваться злоумышленниками.

Дополнительной проблемой является повторное использование паролей в различных информационных системах. В статье [2] рассматриваются организационные проблемы управления учетными данными. Авторы указывают, что сотрудники организаций нередко используют одинаковые пароли для нескольких сервисов, хранят учетные данные в незащищенном виде и применяют общие учетные записи для коллективного доступа.

Особую опасность представляют локальные учетные записи, существующие вне централизованной инфраструктуры управления доступом. Подобные аккаунты зачастую создаются вручную администраторами и не подпадают под действие корпоративных парольных политик. Вследствие этого локальные учетные записи становятся одной из наиболее уязвимых составляющих информационной инфраструктуры организации.

2. Современные методы выявления слабых паролей

Одним из наиболее распространенных подходов к обнаружению слабых паролей является аудит учетных данных с использованием специализированных средств password auditing. Стандартные методы поиска потенциально компрометируемых аутентификационных данных используют алгоритмы поиска по словарям и маскам, алгоритмы полного перебора всех возможных комбинаций, а также словари, содержащие известные скомпрометированные данные. Однако интеллектуальные алгоритмы существенно повышают эффективность современных средств password guessing.

В работе [3] рассматриваются методы подбора паролей, в основе которых используется анализ языковых и региональных особенностей. Авторы демонстрируют, что выбор пароля во многом определяется национальностью пользователя, используемым языком и особенностями конкретного сервиса. На основе подобных закономерностей формируются вероятностные модели, позволяющие значительно повысить эффективность подбора.

В отличие от базовых видов атак современные методы подбора паролей используют также статистический анализ пользовательских сессий. По результатам анализа было установлено, что англоязычные пользователи в большей степени применяют английские слова и распространенные англоязычные конструкции, тогда как пользователи других стран используют имена, даты или другие конструкции, характерные им. Подобные закономерности позволяют успешно выявлять слабые пароли даже в тех случаях, когда они формально удовлетворяют требованиям парольной политики.

Значительное развитие получили методы статистической оценки стойкости паролей. В работе [4] представлен подход PESrank, позволяющий рассчитать вероятность и риск потенциальной компрометации аутентификационных данных злоумышленником. Предложенный авторами подход учитывает такие статистические характеристики, как частота встречаемости шаблонов и зависимости между символами и их последовательностями. Ключевой особенностью такого метода – интерпретируемость результатов. Помимо определения уровня стойкости также указываются и причины принятого решения, что в свою очередь позволяет повысить эффективность механизмов классификации паролей.

В последних исследованиях прослеживается эффективность методов машинного обучения, применяемых для анализа и классификации паролей. Так в работе [5] рассматривается применение алгоритмов машинного обучения для обнаружения ненадежных учетных данных в корпоративной инфраструктуре.

Авторы предлагают использовать модели классификации, способные автоматически определять вероятность компрометации пароля на основе набора признаков. В качестве таких признаков рассматриваются длина пароля, энтропия, наличие словарных элементов, повторяемость символов и статистические характеристики последовательностей. Использование методов машинного обучения позволяет существенно повысить точность обнаружения слабых паролей по сравнению с традиционными правилами парольной политики.

3. Выявление локальных и дефолтных паролей

Одной из существенных проблем в области информационной безопасности остается использование учетных данных по умолчанию. В работе [6] показано, что значительная часть программных и аппаратных решений поставляется со стандартными учетными записями и предустановленными паролями. При этом пользователи зачастую не осуществляют их изменение после ввода системы в эксплуатацию, что приводит к возникновению критических уязвимостей.

Отмечается, что практика использования дефолтных паролей наиболее характерна для сетевого оборудования, встроенных систем и административных интерфейсов. Дополнительную угрозу представляет наличие скрытых локальных учетных записей, о существовании которых администраторы могут не иметь информации.

Локальные учетные записи относятся к категории объектов, представляющих повышенную сложность для централизованного контроля. В отличие от доменных учетных записей, они нередко не подпадают под действие корпоративных политик безопасности и редко подвергаются регулярному аудиту. Вследствие этого для них характерно использование простых или устаревших паролей, сохраняющихся без изменений на протяжении длительного времени.

Для выявления указанных уязвимостей применяются специализированные средства аудита, обеспечивающие анализ локальных баз учетных данных, проверку хэшей паролей, а также сопоставление учетных записей с базами ранее скомпрометированных учетных данных. Дополнительно используются методы автоматизированного анализа конфигураций информационных систем и сетевого оборудования [5].

Современные системы мониторинга информационной безопасности обеспечивают автоматизированное выявление слабых административных паролей и неиспользуемых локальных учетных записей. Применение таких средств позволяет существенно повысить уровень защищенности корпоративной инфраструктуры и снизить вероятность компрометации учетных данных.

Заключение

Использование потенциально компрометируемых аутентификационных данных может нести высокие риски при обеспечении безопасности информационных систем. Несмотря на введение ограничительных мер в виде парольных политик и механизмов верификации, у пользователей остается возможность регистрации учетных записей с ненадежными паролями.

Дополнительные риски несут локальные и системные учетные записи, на которые обычно не распространяются глобальные требования парольных политик. В связи с чем возникает необходимость своевременного обнаружения подобных аутентификационных данных. Для этого необходимо применять специализированные механизмы контроля и аудита, а также интеллектуальные методы анализа данных.

В качестве одного из наиболее перспективных направлений развития систем выявления ненадежных паролей рассматривается применение методов машинного обучения и статистического анализа. Использование данных подходов позволяет повысить эффективность выявления потенциально компрометируемых учетных записей и снизить вероятность компрометации информационных систем, в которых они используются.

Благодарности.

Исследование выполнено за счет гранта Российского научного фонда №25-71-30007, <https://rscf.ru/project/25-71-30007/>.

Литература

1. Yildirim M., Mackie I. Encouraging users to improve password security and memorability //International Journal of Information Security. – 2019. – Т. 18. – №. 6. – С. 741-759.
2. Ngandu M. R., Mwansa G., Mkabe Z. Strengthening cybersecurity in a government department by addressing password management challenges and human factor vulnerabilities //Discover Computing. – 2025. – Т. 28. – №. 1. – С. 148.
3. Murray H., Malone D. Adaptive password guessing: learning language, nationality and dataset source //Annals of Telecommunications. – 2023. – Т. 78. – №. 7. – С. 385-400.
4. David L., Wool A. An explainable online password strength estimator //European Symposium on Research in Computer Security. – Cham : Springer International Publishing, 2021. – С. 285-304.

5. Rusanov M. et al. Identification of exploited unreliable account passwords in the information infrastructure using machine learning methods //Big Data and Cognitive Computing. – 2024. – Т. 8. – №. 11. – С. 159.
6. Knieriem B. et al. An overview of the usage of default passwords //International Conference on Digital Forensics and Cyber Crime. – Cham : Springer International Publishing, 2017. – С. 195-203.

WEAK PASSWORDS AS A FACTOR OF ACCOUNT COMPROMISE: MODERN METHODS OF DETECTION AND ANALYSIS

PhD student Rusanov M.A., PhD associate professor Lapina M.A.

North-Caucasus Federal University, Stavropol

The paper presents an overview of modern methods for identifying weak passwords in organizational information systems. The main reasons for the use of unreliable passwords are considered, including the human factor, limitations of traditional password policies, password reuse, and the presence of local user accounts. An analysis of existing approaches to weak password detection based on dictionary attacks, statistical models, password guessing methods, and machine learning algorithms is carried out. Particular attention is paid to the problem of default and local passwords that are not covered by centralized security policies. Modern methods for assessing password strength and approaches to improving the effectiveness of account protection are examined. It is concluded that the use of intelligent analysis methods and machine learning is a promising direction for the automated detection of vulnerable passwords in corporate infrastructure.



РАННЕЕ ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК ПОСРЕДСТВОМ АНАЛИЗА СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

д.т.н. доц. Щербаков В.А., студ. Селюшкин М.А.

Национальный исследовательский университет «МИЭТ»

В работе рассматривается вопрос возможных направлений применения нейронных сетей в интересах обеспечения информационной безопасности. Показано, что традиционные сигнатурные методы не обеспечивают необходимой эффективности в условиях роста сложности и скрытности угроз информационной безопасности. Описаны подходы к подготовке данных, выделению информативных признаков и построению моделей глубокого обучения нейронной сети. Особое внимание уделено гибридной архитектуре CNN-LSTM, позволяющей учитывать как пространственные, так и временные зависимости сетевого трафика. Приведен пример, описывающий возможность использования нейросетевых методов для выявления атак на ранних стадиях.

В условиях цифровой трансформации критической инфраструктуры и массового перехода к облачным вычислениям наблюдается экспоненциальный рост сложности, скрытности и автоматизации компьютерных атак. По некоторым данным [1], среднее «время прорыва» сократилось до 29 минут, а самый быстрый случай составляет всего 27 секунд. При этом число атак с использованием искусственного интеллекта (ИИ) выросло на 89%, (рисунок 1), также 82% всех обнаруженных угроз вовсе не использовали классическое вредоносное ПО.



Рисунок 1 – Статистика применения ИИ в интересах реализации кибератак

Применяемые в настоящее время методы обнаружения вторжений, основанные на анализе сигнатур или пороговых значений статистических параметров, демонстрируют недостаточную эффективность. Актуальной задачей становится разработка систем, способных осуществлять раннее обнаружение атак на основе анализа аномалий в поведении сетевого трафика. При этом ручной анализ трафика сталкивается с критическими ограничениями: огромные объёмы данных, высокая скорость их поступления, необходимость круглосуточного мониторинга и риск пропуска скрытых аномалий из-за человеческого фактора. Человек не способен в реальном времени отслеживать тысячи параллельных потоков и выявлять микроскопические отклонения в статистике пакетов, что делает автоматизацию процесса критически необходимой задачей.

Для решения данной задачи перспективным решением является переход к поведенческим системам обнаружения аномалий, использующим методы глубокого обучения.

Целью данной работы служит анализ возможности применения нейронных сетей различной архитектуры для задач раннего обнаружения компьютерных атак, а также описание подхода к подготовке сетевых данных, выделению информативных признаков и построению эффективной архитектуры модели обнаружения.

Для решения этой цели были поставлены следующие частные задачи:

1. Провести анализ опыта применения нейронных сетей для решения задач в области сетевой и информационной безопасности.
2. Выполнить сравнительный анализ существующих архитектур нейронных сетей, применяемых в задачах сетевой безопасности.
3. Описать этапы предварительной обработки сетевых данных, включая методы нормализации, кодирования категориальных переменных данных.
4. Выявить и классифицировать ключевые признаки сетевого трафика, наиболее чувствительные к различным типам атак.
5. На примере атаки типа DDoS продемонстрировать механизм работы нейросетевой модели, показать, как временные и статистические зависимости используются для раннего принятия решения о наличии угрозы.
6. Оценить качество работы модели на стандартизированном наборе данных с использованием различных метрик.

Применение методов машинного обучения в задачах информационной безопасности берёт начало в 1990-х годах, однако массовое внедрение нейросетевых подходов началось в середине 2010-х годов, после прорыва архитектур глубокого обучения в компьютерном зрении.

Одними из первых считаются работы Р. Липпманна, предложившего использовать нейронные сети для классификации сетевого трафика [2]. Современный опыт применения показывает, что нейронные сети (НС) могут использоваться даже для повышения защищенности атомных электростанций [3].

Ключевой особенностью применения искусственного интеллекта в сетевой безопасности является переход от сигнатурной защиты к проактивному поведенческому анализу. ИИ не ищет известные шаблоны вредоносного кода, а изучает состояние системы и фиксирует отклонения от нормы. Это позволяет реагировать на атаки, которые ещё не описаны в базах сигнатур.

Однако важно понимать границы применимости нейросетей:

к атакам, эффективно обнаруживаемым нейросетями, относятся DDoS, сканирование портов, перебор учётных данных, аномальные всплески трафика, подозрительные сессии командных серверов, попытки эксплуатации уязвимостей с характерными статистическими аномалиями в заголовках пакетов;

к атакам, обнаружение которых затруднено или невозможно без дополнительных контекстных данных, относятся целевой фишинг на уровне социальной инженерии, атаки с полным шифрованием полезной нагрузки при отсутствии метаданных, физические атаки на инфраструктуру, а также сложные многоэтапные АРТ-атаки с крайне низкой скоростью.

Прежде чем перейти к сравнению конкретных архитектур, необходимо определить, как именно нейросети применяются в контексте анализа трафика. Основная задача системы обнаружения вторжений на базе нейронных сетей – непрерывная классификация потоков в реальном времени. Для этого данные преобразуются в многомерные массивы, подаются на вход модели, которая возвращает вероятность принадлежности потока к классу «норма» или «атака».

В зависимости от типа данных выбирается подход: если важны локальные шаблоны в байтах пакета – используются сверточные нейросети; если критична последовательность событий во времени – рекуррентные; если стоит задача выявить неизвестные аномалии, то используются автоэнкодеры. Наибольшую эффективность на практике демонстрируют гибридные архитектуры, объединяющие сильные стороны отдельных подходов. Сравнительная характеристика основных архитектур, применяемых в СОВ, представлена в таблице 1 [4].

Таблица 1

Сравнительная характеристика основных архитектур, применяемых в СОВ

Архитектура	Преимущества	Недостатки	Применимость
Сверточные нейронные сети (CNN)	Высокая скорость, устойчивость к шуму	Не учитывает временные зависимости	Анализ пространственных признаков
Рекуррентные нейронные сети (LSTM)	Учёт временных последовательностей	Высокая вычислительная сложность	Раннее обнаружение атак
Autoencoder	Обнаружение неизвестных атак	Много ложных срабатываний	Аномалии нулевого дня

CNN-LSTM	Комбинация преимуществ	Сложность настройки	Универсальное решение
----------	------------------------	---------------------	-----------------------

Сравнительный анализ демонстрирует, что ни одна из базовых архитектур не является универсальной. Сверточные НС эффективны для фильтрации шума, но не показательны во временных зависимостях, в то время как рекуррентные НС их учитывают, но требуют значительных ресурсов. Гибридная модель нивелирует эти недостатки, обеспечивая баланс между скоростью обработки и глубиной анализа, что обосновывает её выбор в качестве базовой для задач раннего обнаружения.

Ключевым этапом построения системы обнаружения атак на основе нейронных сетей является подготовка данных. Качество работы модели напрямую зависит от репрезентативности входной выборки. В качестве основы для обучения и тестирования в работе используется набор данных CIC-IDS2017, содержащий профили реалистичного сетевого трафика с размеченными атаками различных классов [5]. Процесс предобработки данных включает четыре последовательных этапа, представленных на рисунке 2.



Рисунок 2 – Этапы предобработки данных

1. На **первом этапе** удаляются дублирующие записи, обрабатываются пропущенные значения (NaN) путем замены на медианные показатели по каждому признаку.

2. На **втором этапе** категориальные переменные (протоколы, типы служб, TCP-флаги) преобразуются в числовой формат, обеспечивающий корректную интерпретацию признаков нейросетью.

3. **Третий этап** – нормализация числовых признаков, приводящая все признаки к диапазону [0, 1]. Это критически важно для стабилизации градиентного спуска при обучении глубоких архитектур. Нормализация производится по формуле [4]:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}, \quad (1)$$

где X – исходное значение, X_{min} – минимум в выборке, X_{max} – максимум в выборке.

4. На **четвертом этапе** решается проблема сильного дисбаланса классов, характерного для сетевых данных (доля атак составляет менее 5%). Для генерации синтетических примеров миноритарного класса применяется алгоритм SMOTE, который создает новые объекты в пространстве признаков путем интерполяции к ближайшим соседям, что повышает чувствительность модели к редким типам вторжений [4].

После подготовки данных формируется вектор признаков, подаваемый на вход нейросети. Анализ набора данных CIC-IDS2017 и современных исследований по отбору параметров позволяет выделить группы наиболее информативных характеристик потока. К базовым признакам относятся IP-адреса источника и назначения, порты, протокол уровня транспортировки. Статистические признаки потока включают: длительность соединения, интенсивность передачи данных, средний размер пакетов в прямом направлении. Временные характеристики, такие как среднее и суммарное время межпакетных интервалов, а также флаги TCP, отражают динамику установления и разрыва соединений.

Именно эти параметры формируют «отпечаток» поведения узла в сети и используются нейросетью для вычисления аномальности.

Для разработки и интеграции нейросетевой модели в реальную инфраструктуру необходимо определить её место в сетевой топологии. На схеме корпоративной сети модуль обнаружения атак целесообразно развернуть в точке агрегации трафика, например на уровне ядра, или непосредственно перед периметровым межсетевым экраном. Нейросеть не размыкает канал, а работает в режиме пассивного мониторинга через порт зеркального копирования (SPAN) или сетевой отвод (TAP). Архитектурно система может строиться по принципу клиент-сервер или микросервисов: агенты сбора трафика передают потоки в контейнеризованный сервис инференса, который возвращает вердикт в SIEM-систему для автоматического блокирования через API шлюза.

Развёртывание на инфраструктуре организации возможно в нескольких форматах:

1. Установка на выделенные GPU-серверы или CPU-кластеры внутри ЦОД компании, что гарантирует полный контроль над данными.
2. Запуск как виртуальной машины или контейнера в частном облаке, что упрощает масштабирование и резервирование.
3. Оптимизированная (квантованная) версия модели разворачивается на маршрутизаторах или коммутаторах уровня доступа.

Пример развёртывания нейросети по первому формату представлен на рисунке 3.

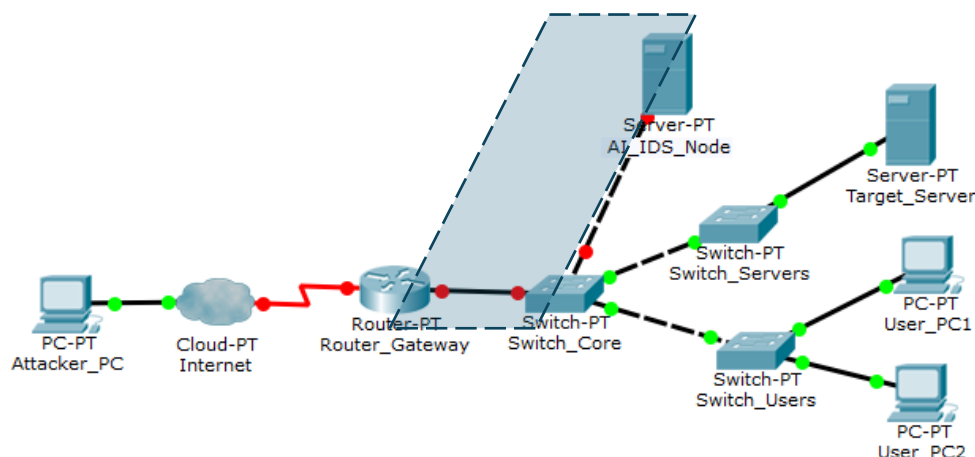


Рисунок 3 – Схема развёртывания нейросети в корпоративной сети

Для понимания механизмов раннего обнаружения необходимо рассмотреть типичные этапы реализации сетевой атаки. В экспертном сообществе сложилось представление о том, что целевая атака, как правило, в своём развитии проходит через 4 фазы [6]. Данные фазы атаки представлены на рисунке 4.



Рисунок 4 – Жизненный цикл компьютерной атаки

Традиционные сигнатурные СОВ активируются преимущественно на этапах эксплуатации уязвимости и действиях на цель, когда атака уже сформирована и несет явные вредоносные признаки. Нейросетевые модели, напротив, способны выявлять аномалии на начальных фазах – разведке и доставке. Например, при сканировании портов НС фиксирует резкое увеличение интенсивности передачи данных и аномальное распределение суммарного времени межпакетных интервалов при отсутствии полезной нагрузки. При подготовке к DDoS-атаке модель обнаруживает синхронный рост SYN-пакетов и сокращение длительности соединения с множественных узлов к одному целевому IP. Таким образом, анализ временных и статистических зависимостей на уровне первых 5-10 пакетов потока позволяет классифицировать активность как враждебную до перехода атакующего к фазе эксплуатации, что и обеспечивает эффект раннего обнаружения.

В качестве практического примера рассмотрим механизм раннего обнаружения DDoS-атаки типа SYN-флуд. Подробная схема взаимодействия при данном типе атаки представлена на рисунке 5.

Традиционные сигнатурные системы обнаруживают атаку лишь на этапе заполнения очередей соединений, когда сервис уже деградировал или стал недоступен.

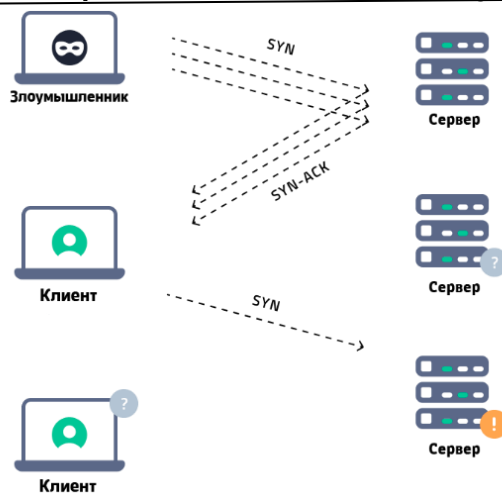


Рисунок 5 – Схема проведения атаки типа DDoS

Нейросетевой подход позволяет идентифицировать угрозу на стадии формирования потока. Модель анализирует скользящее временное окно из первых 5–10 пакетов соединения, извлекая признаки: соотношение SYN/ACK пакетов, скорость появления новых потоков, среднее время межпакетных интервалов и длину пакетов в прямом направлении. Аномальное снижение среднего времени межпакетных интервалов при одновременном экспоненциальном росте скорости появления новых потоков и отсутствии ACK-ответов формирует уникальный паттерн, статистически отличающийся от легитимной возрастающей нагрузки. НС фиксирует это отклонение от распределения нормального трафика еще до достижения пороговой нагрузки.

Для изучения реализации описанного механизма была спроектирована гибридная архитектура CNN-LSTM. Входной тензор размерностью (N, F) , где N – длина временного окна, F – количество признаков, последовательно проходит через два одномерных сверточных слоя (Conv1D) с ядрами размером 3 и функцией активации ReLU. За ними следуют слои MaxPooling для снижения размерности и выделения инвариантных локальных паттернов. Далее данные передаются в рекуррентный блок из двух слоев LSTM по 64 нейрона, который моделирует временные зависимости и запоминает контекст потока [7]. Завершает архитектуру полносвязный слой с функцией активации Sigmoid, выдающий вероятность принадлежности входного потока к классу «атака». Полная схема применяемой архитектуры приведена на рисунке 6.

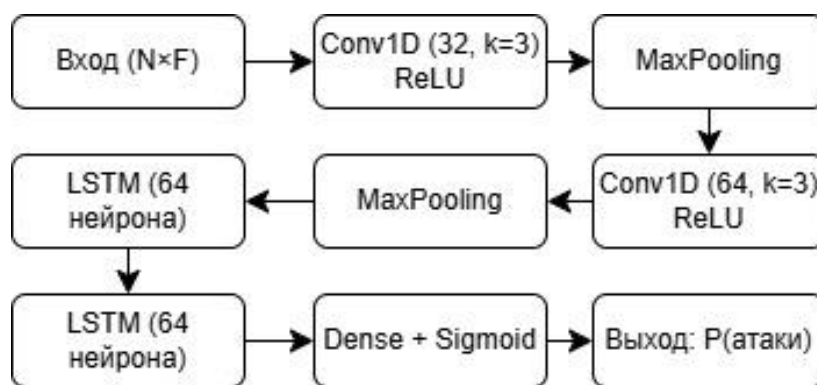


Рисунок 6 – Архитектура гибридной нейросети CNN-LSTM для обнаружения атак

Обучение проводилось на 70 % выборки датасета CIC-IDS2017 с использованием функции потерь Binary Cross-Entropy, BCE (2) и оптимизатора Adam (learning rate = 0.001) [8].

$$BCE = -\frac{1}{N} \sum_{i=1}^N [y_i \times \ln(\hat{y}) + (1 - y_i) \times \ln(1 - \hat{y})], \quad (2)$$

где N – количество примеров в выборке;

y_i – истинная метка класса для i -го примера (0 или 1);

$\hat{y}$ – предсказанная моделью вероятность того, что пример относится к классу 1 (значение от 0 до 1).

Модель продемонстрировала высокую эффективность во всех классах рассматриваемых угроз. Результаты обнаружения НС возможных атак представлены в таблице 2.

Анализ метрик показывает, что значение Recall для DDoS составило 0,97, что важно для задач безопасности: система пропускает менее 3% атак.

Таблица 2

Результаты обнаружения НС рассматриваемых типов атак

Тип атаки	Precision	Recall	F1	Accuracy
Легитимный трафик	0,99	0,99	0,99	0,99
DDoS	0,98	0,97	0,97	0,98
Сканирование портов	0,96	0,95	0,95	0,96
Полный перебор	0,94	0,93	0,93	0,94

Высокое значение Precision свидетельствует о минимальном количестве ложных срабатываний, что снижает нагрузку на аналитиков. Сравнение с базовыми моделями показало прирост F1 на 6-9% за счет совместного использования пространственной фильтрации и временного моделирования. Среднее время изучения одного потока не превышало 4,2 мс на стандартном процессоре, что позволяет интегрировать модель в высокоскоростные сетевые шлюзы для работы в режиме реального времени.

Практическое применение нейросетевых СОВ сталкивается с рядом вызовов. Во-первых, сетевой трафик подвержен дрейфу концепций: легитимное поведение пользователей и протоколы со временем изменяются, что требует периодического дообучения модели на актуальных данных. Во-вторых, атакующие могут применять техники состязательного машинного обучения, добавляя малозаметный шум к признакам пакетов для обхода классификатора. Для противодействия этим угрозам перспективным направлением является внедрение механизмов активного обучения и федеративного обучения, позволяющего обновлять веса модели без передачи конфиденциального трафика в центральный узел.

Таким образом, в ходе работы проведена оценка возможности применения нейронных сетей для анализа сетевого трафика, с целью раннего обнаружения компьютерных атак. Практическая значимость работы заключается в трёх ключевых результатах:

1. Обоснована возможность применения НС: подтверждено, что традиционные сигнатурные методы не справляются с современными угрозами, тогда как поведенческие нейросетевые подходы позволяют оперативно обнаруживать аномалии на ранних стадиях.
2. Обоснован выбор рациональной архитектуры: на основе сравнительного анализа и экспериментальных метрик показано, что CNN-LSTM обеспечивает наилучший баланс между точностью, устойчивостью к шуму и способностью учитывать временные зависимости.
3. Разработан структурный сетевой конструктив: предложена архитектура развёртывания модуля обнаружения в корпоративной сети (режим SPAN/TAP, контейнеризация, интеграция с SIEM), а также описаны сценарии адаптации модели под различные типы инфраструктуры.

Перспективными направлениями дальнейших исследований являются: оптимизация архитектуры модели для развёртывания на периферийных устройствах, внедрение механизмов активного обучения для адаптации к дрейфу концепций, а также исследование устойчивости нейросетевых СОВ к атакам состязательного машинного обучения.

Литература

1. Global Threat Report 2026 [Электронный ресурс] // CrowdStrike. — URL: <https://www.crowdstrike.com/explore/2026-global-threat-report> (дата обращения: 09.04.2026).
2. The 1999 DARPA off-line intrusion detection evaluation [Текст] / R. P. Lippmann, J. W. Haines, D. J. Fried et al. // Computer Networks : internetworking and telecommunications systems. – 2000. – Vol. 34, No. 4. – P. 579–595.
3. Lee S., Huh J.-H., Kim Y. Python TensorFlow Big Data Analysis for the Security of Korean Nuclear Power Plants [Электронный ресурс] // Electronics. – 2020. – Vol. 9, No. 9. – Art. 1467. – DOI:

10.3390/electronics9091467. – URL: <https://doi.org/10.3390/electronics9091467> (дата обращения: 09.04.2026).

4. Vinayakumar R., Alazab M., Soman K. P. Deep Learning Approach for Intelligent Intrusion Detection System [Текст] // IEEE Access. – 2019. – Vol. 7. – P. 41525–41550.
5. Sharafaldin I., Lashkari A. H., Ghorbani A. A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization [Текст] // Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP). – 2018. – P. 108–116.
6. Анатомия целевой атаки [Электронный ресурс] // IT Security. — URL: <https://lib.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki> (дата обращения: 09.04.2026).
7. Ahmed F., Noor D., Saad M. Early DDoS Attack Detection Using Lightweight Deep Neural Network [Текст] // Fusion: Practice and Applications. – 2025. – Vol. 19, No. 2. – P. 392–401. – DOI: 10.54216/FPA.190228.
8. Ayyıldız P., Karahan O. Hyperparameter Optimization for A Hybrid CNN-LSTM-based Intrusion Detection System [Текст] // SETSCI Conference Proceedings. – 2024. – Vol. 17. – P. 7–12.

EARLY DETECTION OF CYBER ATTACKS VIA NETWORK TRAFFIC ANALYSIS USING NEURAL NETWORKS

Dr. Sci., Assoc. Prof. Shcherbakov V.A., stud. Selyushkin M.A.

National Research University of Electronic Technology

This paper explores potential applications of neural networks in information security. It demonstrates that traditional signature-based methods lack sufficient efficiency against increasingly complex and stealthy threats. The study describes approaches to data preprocessing, feature extraction, and the development of deep learning models. Particular emphasis is placed on a hybrid CNN-LSTM architecture capable of capturing both spatial and temporal dependencies in network traffic. An illustrative example highlights the potential of neural network-based methods for early-stage attack detection.



Python и нормализацию кропов до размера 64x64 пикселя в градациях серого. Сформированный датасет был разделен на обучающую (14632 изображения) и тестовую (3955 изображений) выборки. Выборка является несбалансированной. Гистограмма распределения классов обучающей выборки приведена на рисунке 2.

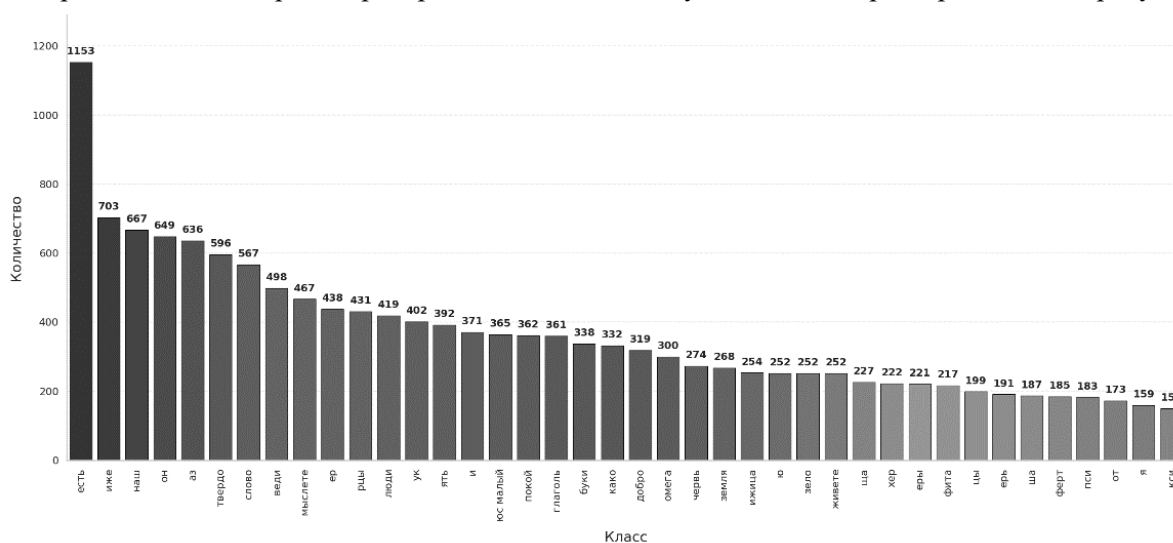


Рисунок 2. Гистограмма распределения классов обучающей выборки

Экспериментально установлено, что глобальная бинаризация методом Оцу приводит к снижению метрик качества из-за потери тонких элементов штрихов (см. таблицу 1). Сравнение шести адаптивных методов показало, что наилучшим является метод Wolf-Jolion. Однако модели, обученные на полутоновых изображениях, сохраняют более высокую обобщающую способность (Ассигасу 95,723% против 90,835% у бинаризованных для yolol1m). Поэтому дальнейшие исследования проводились на данных в градациях серого.

Для решения проблемы дисбаланса классов применялась геометрическая аугментация (малые повороты, сдвиги, масштабирование). Она показала стабильный прирост точности. Для yolov8m оптимальный результат достигнут при 10000 изображениях на класс (ассигасу = 97,759%), для yolol1m — при 2000 изображениях на класс (ассигасу = 98,167%).

Применение генеративно-сопоставительных сетей, включая AC-GAN, BAGAN-lite, ReACGAN и ADCGAN, оказалось менее эффективным. Синтез новых символов сопровождался частичным коллапсом мод, нестабильностью обучения и нарушением классовой обусловленности генерации на малых выборках. Контролируемая геометрическая аугментация показала себя более надежным подходом.

На базе лучшей конфигурации исследовалось влияние параметров оптимизации. Оптимальной конфигурацией стал оптимизатор SGD с начальным шагом обучения 0.001 и коэффициентом регуляризации 0.0005.

Для апробации разработанных подходов реализован программный комплекс в формате интерактивного Telegram-бота. Сервис выполняет предобработку скан-копий, сегментацию строк и графем с использованием алгоритма водораздела [4] и последующую классификацию каждого символа моделью yolol1m-cls. Пример работы представлен на рисунке 3.

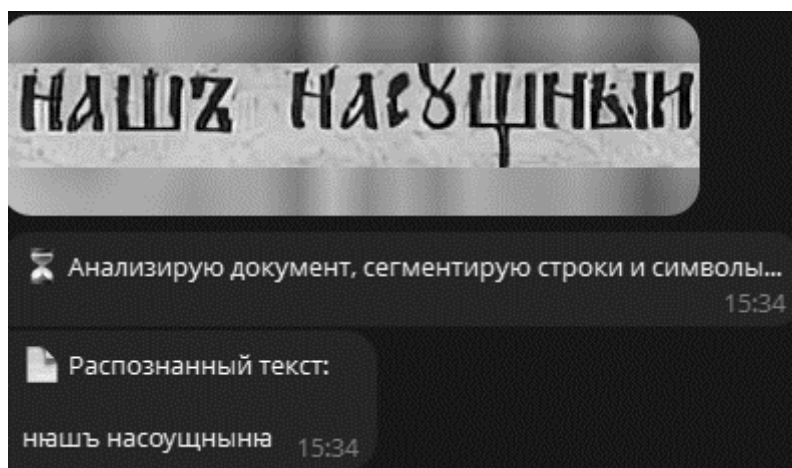


Рисунок 3. Пример работы Telegram-бота

Проведенное исследование подтверждает гипотезу о том, что итоговое качество распознавания старославянских рукописных символов в большей степени определяется стратегией подготовки данных, грамотной аугментацией и настройкой параметров, нежели выбором конкретной архитектуры внутри современного семейства YOLO. Перевод в градации серого оказался эффективнее бинаризации, а контролируемые геометрические преобразования превзошли генеративные подходы на базе GAN по надежности и качеству итоговой классификации.

Литература

1. Хабургаев, Г. А. Старославянский язык [Текст] / Г. А. Хабургаев. — 2-е изд., перераб. и доп. — Москва: Просвещение, 1986.
2. Мамедов, Т. Р. Распознавание исторических рукописных документов с применением методов глубокого машинного обучения [Текст] / Т. Р. Мамедов, Н. М. Ершов // Системный анализ в науке и образовании. — 2024. — № 3. — С. 46-53.
3. Terven, J. A Comprehensive Review of YOLO Architectures in Computer Vision: From YOLOv1 to YOLOv8 and YOLO-NAS [Текст] / J. Terven, D. Cordova-Esparza // Machine Learning and Knowledge Extraction. — 2023. — Vol. 5, no. 4. — P. 1680-1716.
4. Власов, Д. А. Проблемы и методы сегментации и распознавания символов в задачах оцифровки архивных документов [Текст] / Д. А. Власов, Ю. В. Визильтер // Вестник компьютерных и информационных технологий. — 2021. — № 5. — С. 12-20.

DEVELOPMENT AND COMPARATIVE ANALYSIS OF ADAPTED PRE-TRAINED MODELS FOR OLD SLAVIC HANDWRITTEN CHARACTER RECOGNITION

stud. Ryabov D. A.

Ulyanovsk State Technical University

This paper addresses the problem of automatic recognition of historical handwritten texts at the level of individual Old Slavic characters. An experimental study and a comparative analysis of YOLO family classification models (yolov8m-cls and yolov11m-cls) were conducted. The study evaluates the impact of data preparation methods—including binarization, geometric augmentation, and generative sample expansion using GANs—on the final classification accuracy. It is demonstrated that the geometric augmentation of grayscale images, combined with the optimization of training hyperparameters, ensures the best generalization capability of the models. The practical significance of this work is confirmed by the development of an interactive Telegram bot for the segmentation and recognition of historical documents.



ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ВЗАИМНОЙ ИНФОРМАЦИИ В КАЧЕСТВЕ ЦЕЛЕВОЙ ФУНКЦИИ В СТОХАСТИЧЕСКИХ АЛГОРИТМАХ СОВМЕЩЕНИЯ РАЗНОСПЕКТРАЛЬНЫХ И РАЗНОВРЕМЕННЫХ ИЗОБРАЖЕНИЙ

проф. Ташлинский А.Г., ассист. Ибрагимов Р.М.

Ульяновский государственный технический университет,

Рассмотрена эффективность релейных стохастических алгоритмов привязки разнотональных и разновременных изображений, синтезированных на основе трех целевых функций качества совмещения: среднего квадрата разности яркостей, кросс-корреляции и взаимной информации Ренни изображений. Показано, что применение среднего квадрата разности яркостей для этого класса изображений неэффективно. Алгоритм на основе кросс-корреляции справляется только с разнотональными изображениями относительно близкого спектра, но не эффективен при разновременных изображениях с большим уровнем нелинейных яркостных искажений. Алгоритм на основе ВИ Ренни на всех типах исследованных изображений показал устойчивые результаты совмещения.

Постановка задачи, выбор алгоритмов

Совмещение изображений, заданных дискретными сетками отсчетов, одна из востребованных процедур при их обработке. Необходимость решения этой задачи возникает в самых различных приложениях: комплексировании разнородных снимков в медицине [1], отслеживании по видеоинформации динамики изменений элементов промышленных объектов [2], построении траекторий беспилотных летальных и подводных аппаратов [3], мониторинге земной поверхности, обнаружении объектов интереса [4] и многих других. Математически задача сводится к установлению соответствия между сопряженными точками двух и более изображений.

При совмещении разновременных и разнотональных изображений возникают дополнительные проблемы, которые обусловлены тем, что кроме различных времени, ракурса и масштаба съемки, они могут отличаться значительными нелинейными яркостными искажениями и импульсными помехами априорно неизвестного вида. Классические алгоритмы совмещения изображений, например, SIFT [5] и SURF [6] в этом случае малоприменимы. Алгоритмы, использующие реперные отметки [7], основанные на разбиении изображений на фрагменты, с использованием секвентного анализа [8] в сложных условиях имеют низкую точность и достоверность совмещения. Лучшую устойчивость оценок в этих условиях обеспечивают алгоритмы псевдоградиентного совмещения изображений [9]. Широкое применение нашли безыдентификационные псевдоградиентные алгоритмы. Их синтез основан на мерах подобия изображений, которые используются как целевые функции качества оценивания параметров совмещения. Решение сводится к итерационному поиску в пространстве параметров экстремума многомерной целевой функции [10].

Значительная априорная неопределенность при привязке разновременных и разнотональных изображений накладывает дополнительные требования к мерам подобия, на основе которых эти изображения совмещаются. В последнее время растет интерес к теоретико-информационным мерам, в частности, взаимным информации Шеннона [11], Ренни [12] и Тсаллиса [13]. Их использование в реальных прикладных задачах длительное время сдерживалось вычислительной трудоемкостью. Однако развитие вычислительных средств и эффективные приемы нахождения аппроксимаций плотностей распределения вероятностей (ПРВ) яркостей изображений это препятствие устранили.

В работе исследуется сравнительная эффективность алгоритмов привязки разновременных и разнотональных изображений, построенных на основе трех мер подобия изображений: средний квадрат разности яркости привязываемых изображений (СКЯ), коэффициент кросс-корреляции изображений (ККИ) и взаимная информация (ВИ) Ренни. Для синтеза алгоритмов использован математический аппарат безыдентификационной псевдоградиентной адаптации [9]. Использовались релейные стохастические алгоритмы [14], которые в условиях априорной неопределенности показали высокую устойчивость. В качестве модели геометрических деформаций применена модель подобия [15], включающая параметры сдвига по базовым осям изображений, угла поворота и коэффициента масштаба.

Результаты экспериментальных исследований

Экспериментальное исследование проводилось на имитированных и реальных изображениях. В качестве смоделированных использовались изображения, полученные на основе волновой модели [16]. Пример такого изображения приведен на рисунке 1а. Достоинством таких имитированных изображений является то, что ПРВ их яркостей (рисунок 2а) и автокорреляционная функция близки к гауссовым. Поэтому их применение позволяет корректно проверить адекватность аналитических результатов, полученных в предположении гауссовой ПРВ яркостей и автокорреляционной функции изображений.

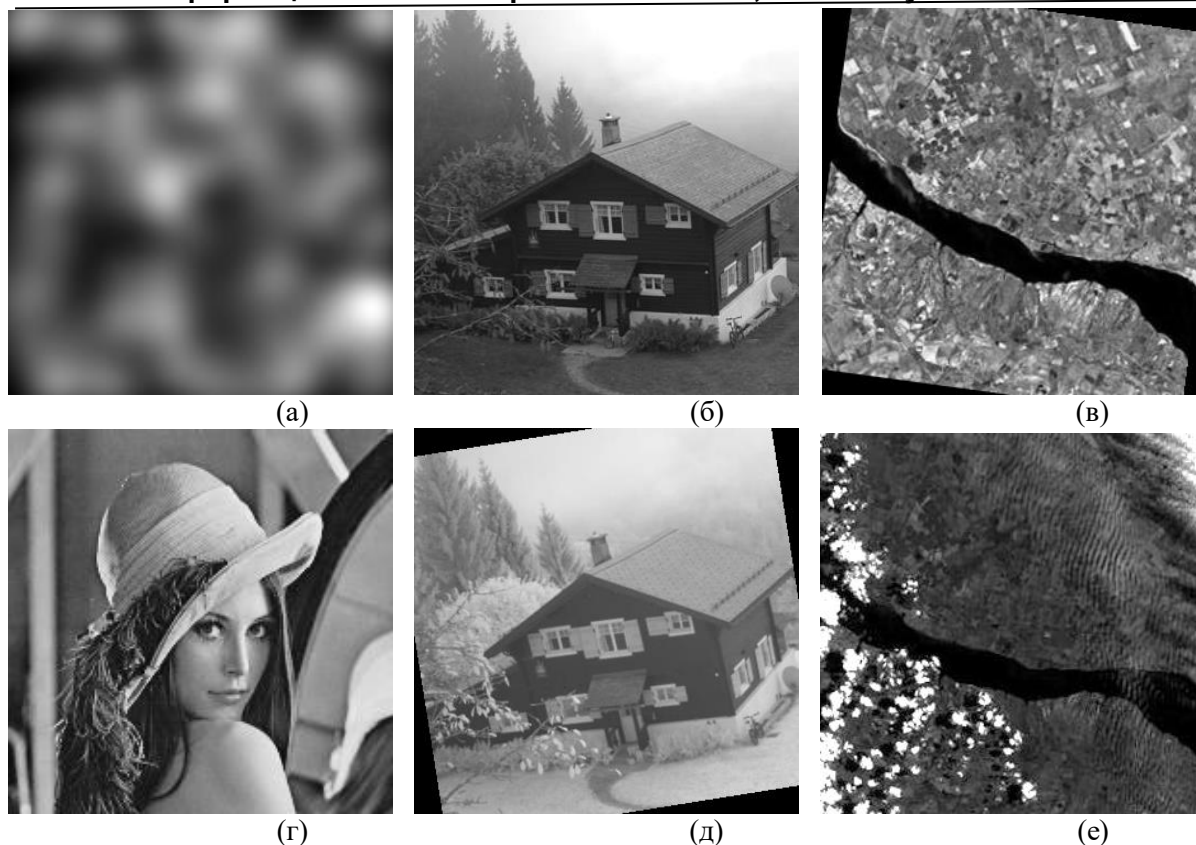


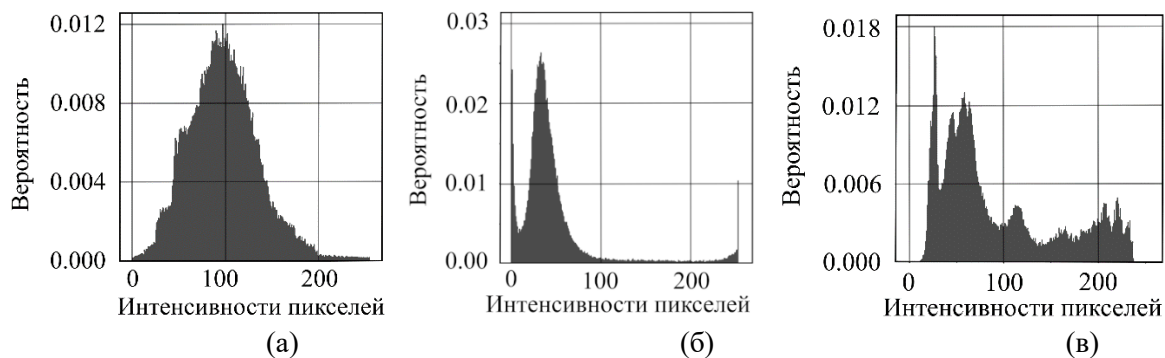
Рисунок 1. Примеры исследуемых изображений

Одновременные изображения видимого диапазона

Кроме разновременных и разносектральных изображений для сравнения как наиболее благоприятная ситуация использовались также изображения видимого диапазона, у которых деформированное изображение получено из опорного моделированием деформаций. На рисунке 1г приведено одно из таких изображений, а на рисунке 2г – его ПРВ яркостей, которая уже значительно отличается от гауссовой.

Пример результатов оценивания алгоритмами, разработанными на основе СКЯ, ККИ и ВИ Реньи изображения рисунка 1г, для ситуации, когда деформированное изображение отличается от опорного поворотом на 9° , приведен на рисунке 3, где рисунок 3а показаны зависимости от ОЛВ дисперсии оцениваемого параметра, а на рисунке 3г – числа итераций сходимости. Результаты усреднены по 30 реализациям. Кривые 1 соответствуют использованию СКЯ, 2 – ККИ, 3 – ВИ Реньи. Отметим, что для сравнимости результатов здесь и в следующих приведенных примерах деформация и число реализаций были аналогичными.

Число итераций сходимости, характеризующее быстродействие алгоритма – это числа итераций, необходимых для достижения установившегося режима оценивания, который определяется тем, что изменение среднего значения оценок в скользящем окне заданного размера не превышает заданного порога. Размер окна и порог выбирался исходя из вероятности ошибки первого рода гипотезы, что математическое ожидание оценки достигло её оптимального значения. В том же окне считается и оценка дисперсии оценок параметров деформаций.



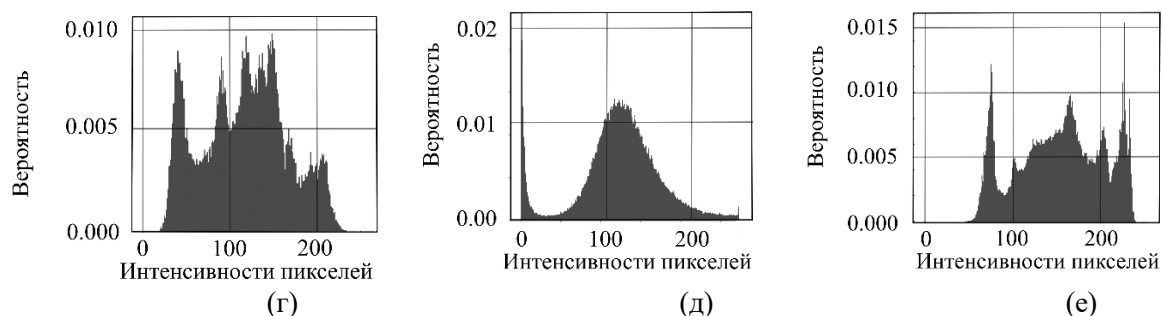


Рисунок 2. ПРВ видимого диапазона, разнспектральных и разновременных изображений

Из рисунков 3а и 3г видно, что в «благоприятном» случае наибольшее быстроедействие обеспечивает СКЯ, потом ККИ и ВИ Реньи. Дисперсия погрешности оценок параметра также минимальна при СКЯ. Но ККИ по точности проигрывает ВИ Реньи.

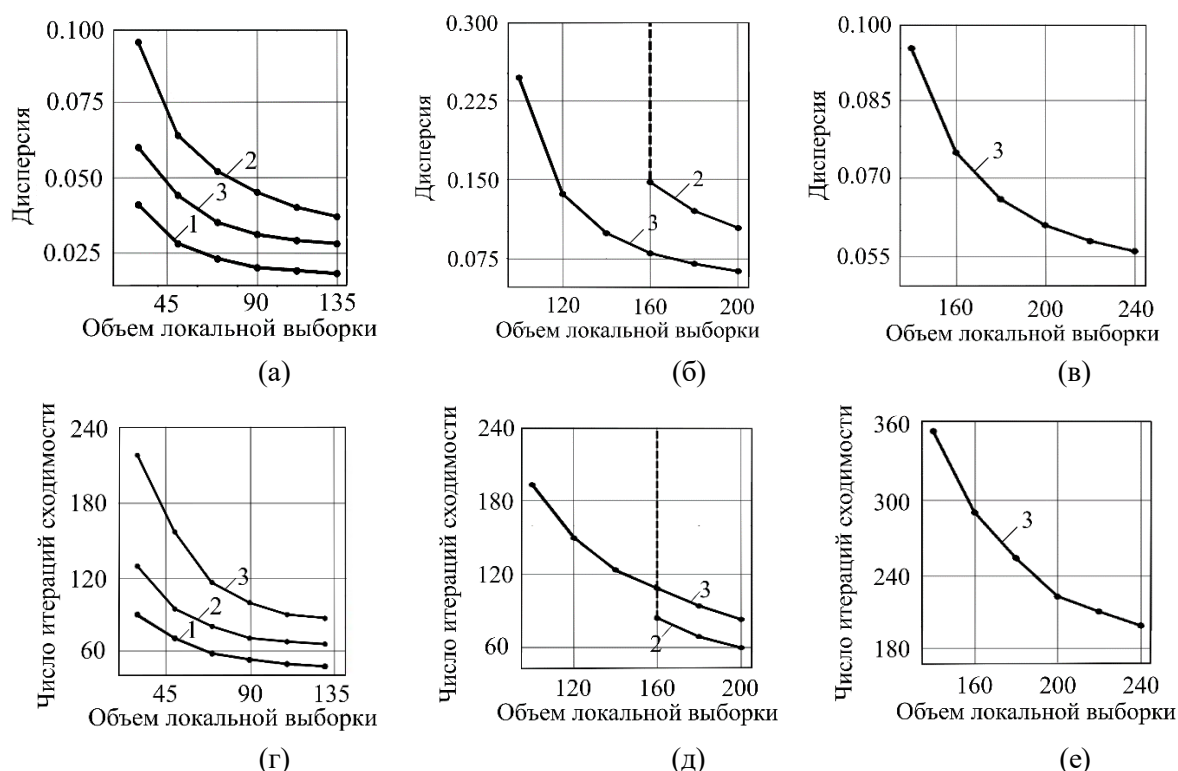


Рисунок 3. Зависимость дисперсии оценок погрешности привязки и числа итераций сходимости от ОЛВ

Разнспектральные изображения

Пример разнспектральных изображений приведен на рисунках 1б (видимый диапазон) и 1д (инфракрасный диапазон). Видно, что ПРВ разнспектральных изображений (рисунки 2б и 2д) несколько схожи по форме, но существенно различаются по вероятностям яркостей. Это делает применение в качестве целевой функции СКЯ нецелесообразным. Проведенные эксперименты подтвердили, что в заданных пределах ОЛВ наблюдались только срывы оценивания. Это же подтверждается и зависимостями СКЯ от сдвига (рисунок 4а,) Видно, что для этого класса изображений СКЯ слабо зависит от сдвига, поэтому погрешность псевдоградиента СКЯ, сравнивая с его величиной, ведет к срыву оценивания. На рисунке 4 кривые 1 соответствуют изображениям видимого спектра, 2 – разнспектральным, 3 – разновременным. приведены нормированная зависимость СКЯ).

В отличие от изображений видимого диапазона, где максимум взаимной корреляционной функции составляет 0,8 (рисунок 4б), для этого класса изображений максимум очень небольшой, равный 0,25, что говорит о том, что для него применение ККИ не может быть эффективным. Поэтому использование в качестве целевой функции ККИ обеспечивало сходимость алгоритма только при ОЛВ большем 160 (рисунки 3б и 3д), где срыв оценивания показан пунктирной линией). Использование ВИ Реньи даёт устойчивую сходимость алгоритма во всем диапазоне ОЛВ с существенно меньшей дисперсией, чем ККИ. Это же подтверждают и зависимости ВИ Реньи от сдвига (рисунок 4в), где прослеживаются выраженные максимумы для всех типов изображений.

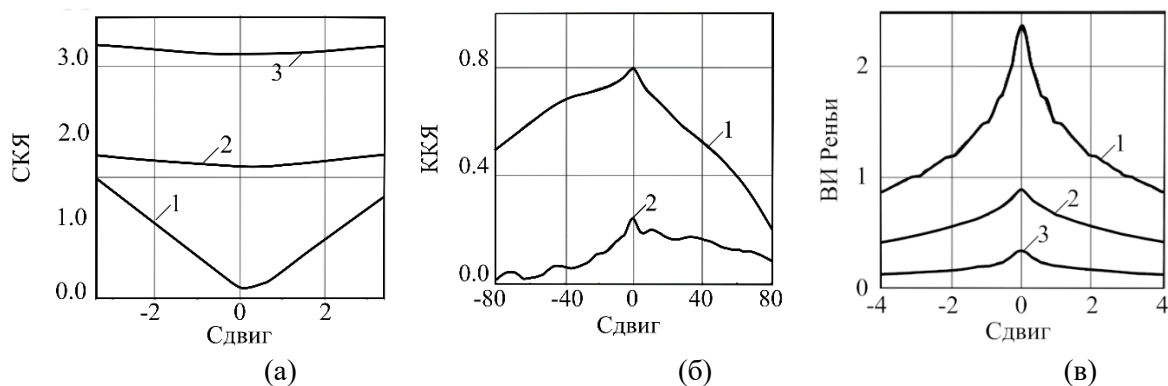


Рисунок 4. Зависимость СКЯ, ККА и ВИ Реньи от сдвига

Разновременные изображения

Пример разновременных спутниковых изображений приведен на рисунках 1в и 1е (снимки реки Волги в апреле 2019 года октябре 2020 в разное время суток). ПРВ этих изображений (рисунки 2в и 2е) уже принципиально различны. Кроме того, зависимость ККА от сдвига не имеет максимума при нулевом сдвиге. Все проведенные эксперименты также показали срывы оценивания. При этом алгоритм на основе ВИ Реньи показал устойчивую сходимость, почти не потеряв в скорости по сравнению с ранее рассмотренными ситуациями.

Заключение

Таким образом, проведенные исследования показали, что использование СКЯ в качестве целевой функции при привязке разносектральных и разновременных изображений не эффективно. Алгоритмы на основе ККА справляются с разносектральными изображениями относительно близкого спектра, но при этом склоны к срывам оценивания. Использование же их для совмещения разновременных изображений с большим уровнем нелинейных яркостных искажений не может быть рекомендовано. Алгоритм на основе ВИ Реньи на всех типах исследованных изображений показал устойчивую сходимость во всем использованном диапазоне ОЛВ. Кроме того, он обеспечивает примерно в 1,4 раза меньшую погрешность оценок параметров привязки, в области, где сходимость алгоритма на основе ККИ достигается.

Исследование выполнено за счет гранта РФФИ № 26-11-10336, <https://rscf.ru/project/26-11-10336>.

Литература

- Fida A.D. Automated combination of optical coherence tomography images and fundus images. *Computer Optics*; 2021, 45(5): 721–727. DOI: 10.18287/2412-6179-CO-892.
- Dementiev V.E., Magdeev R.G. and Tashlinskii A.G. Detecting anomalies in temporal image sequences based on object identification by the stochastic gradient adaptation. *IEEE Conference Proceedings*; 2021; 1-5. DOI: 10.1109/ITNT52450.2021.9649175.
- Камаев А.Н., Карманов Д.А.. Визуальная навигация автономного необитаемого подводного аппарата с глобальным поиском связей между изображениями. *Computer Optics*; 2018; 42(3): 457-467.
- Magdeev R.G., Tashlinskii A.G. Efficiency of object identification for binary images. *Computer Optics*; 2019, 43(2): 277-281.
- Cui Zh., Sheng V.S., Zhao P., Su D., Gong Sh.. A Comparative Study of SIFT and its variants. *Measurement Science Review*; 2013; 13(3): 122-131.
- Bay H., Ess A., Tuytelaars T., Gool L. SURF: Speeded Up Robust Features. *Computer Vision and Image Understanding*; 2008; 110(3): 346-359.
- Гуляев П.В. Применение реперных отметок для координатной привязки к поверхности в сканирующей зондовой микроскопии. *Компьютерная оптика*; 2020; 44(3): 420-426. DOI: 10.18287/2412-6179-CO-641.
- Злобин В.К., Колесников А.Н., Костров Б.В. Корреляционно-экстремальные методы совмещения аэрокосмических изображений. *Вестник Рязанского государственного радиотехнического университета*, т. 37, № 3, с. 12-17, 2011.
- Tashlinskii A.G. Optimization of goal function pseudogradient in the problem of Interframe geometrical deformations estimation. *Pattern Recognition Techniques, Technology and Applications*; 2008; 249-280.

- Wachowiak M.P., Smolikova R., Tourassi G.D. Elmaghraby, Similarity metrics based on nonadditive entropies for 2D-3D multimodal Biomedical image registration. Medical Imaging 2003: Image Processing; 2003: 5032: 1090-1100.
- Shannon C.E., Weaver W. The mathematical theory of communication. Urbana: University of Illinois Press; 1998.
- Rényi A. On measures of entropy and information. Proc. Fourth Berkeley Symposium on Mathematical Statistics Probability; 2006; 1: 547-561.
- Cvejic C.N., Canagarajah D.R. Bull. Image fusion metric based on mutual information and tsallis entropy. Electronics Letters; 2006; 42(11): 626-627.
- Tashlinskii A., Ibragimov R., Safina G.. Application of Renyi Mutual Information in Stochastic Referencing of Multispectral and Multi-temporal Images. 2022 VIII International Conference on Information Technology and Nanotechnology (ITNT); 2022; 1-6. DOI: 10.1109/ITNT55410.2022.9848648.
- Gonzalez R.C., Woods E., Digital image. London: Pearson Publisher; 2018.
- Крашенинников В.Р. Основы теории обработки изображений: Учебное пособие. Ульяновск: УлГТУ; 2003.

EFFICIENCY OF USING MUTUAL INFORMATION AS AN OBJECTIVE FUNCTION IN STOCHASTIC ALGORITHMS FOR COMBINING MULTI-SPECTRAL AND MULTI-TEMPORAL IMAGES

prof. Tashlinskii A.G., lect. Ibragimov R.M.

Ulyanovsk State Technical University

The effectiveness of stochastic relay algorithms for matching multi-spectral and multi-temporal images synthesized using three alignment quality objective functions: mean squared luminance difference, cross-correlation, and Rényi mutual information (MSI). It is shown that using MSI is ineffective for this class of images. The cross-correlation-based algorithm only copes with multi-spectral images of relatively similar spectra, but is ineffective for multi-temporal images with a high level of nonlinear luminance distortion. The MSI-based algorithm demonstrated stable alignment results for all types of images studied.



РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ МНОГОКРИТЕРИАЛЬНОЙ ОПТИМИЗАЦИИ В ПРОГРАММАХ ЛОЯЛЬНОСТИ НА ОСНОВЕ МОДЕЛЕЙ ГЛУБОКОГО ОБУЧЕНИЯ

асп. Яровой А.А.

Финансовый университет при Правительстве Российской Федерации

В работе представлена концепция интеллектуальной системы многокритериальной оптимизации программ лояльности, использующей модели глубокого обучения. Программы лояльности являются ключевым инструментом удержания клиентов в розничной торговле, банковском секторе и телекоммуникациях, однако их эффективность ограничивается сложностью балансирования противоречивых критериев: рентабельности кампаний, удовлетворённости клиентов, частоты покупок и оттока. Предлагаемая система объединяет рекуррентные нейронные сети для прогнозирования поведения клиентов, методы обучения с подкреплением для генерации персонализированных предложений и эволюционные алгоритмы для поиска Парето-оптимальных решений. Архитектура включает модуль сегментации клиентов, модуль предсказания отклика, ядро многокритериальной оптимизации и подсистему обратной связи. Экспериментальная апробация на синтетическом наборе данных показала повышение прогнозируемой удельной выручки на 12–18 % при одновременном росте индекса удовлетворённости клиентов на 6–9 % по сравнению с базовыми моделями.

Введение. В условиях высокой конкуренции на рынках розничной торговли, банковских и телекоммуникационных услуг программы лояльности являются одним из ключевых инструментов формирования долгосрочных отношений с клиентами и повышения экономической эффективности компании. По данным отраслевых обзоров, более 70 % крупных ритейлеров используют те или иные формы поощрения постоянных покупателей. Развитие систем сбора больших данных (Big Data) привело к тому, что компании накапливают терабайты транзакционной информации, однако традиционные аналитические методы не всегда способны извлечь из неё максимальную ценность.

При этом задача формирования персональных предложений и условий начисления бонусов становится всё более сложной: необходимо одновременно учитывать множество неоднородных и зачастую противоречивых критериев — рентабельность кампании, средний чек, частоту покупок, удовлетворённость клиента, вероятность оттока, отклик на коммуникации, выполнение операционных и бюджетных ограничений. Традиционные подходы, основанные на ручной сегментации и эвристических правилах, оказываются неэффективными при количестве клиентов, исчисляемом миллионами, и пространстве возможных предложений, оцениваемом миллиардами комбинаций.

В связи с этим актуальной является разработка интеллектуальной системы многокритериальной оптимизации (МКО), способной адаптивно подбирать персонализированные параметры программы лояльности с учётом всего множества целевых показателей. В докладе предлагается архитектура такой системы, основанная на совместном применении моделей глубокого обучения, методов обучения с подкреплением и эволюционных алгоритмов многокритериальной оптимизации.

Постановка задачи. Формализуем задачу персонализации. Пусть имеется множество клиентов $C = \{c_1, \dots, c_N\}$ и множество возможных предложений (бонусные ставки, скидки, баллы, кэшбэк, целевые коммуникации) $A = \{a_1, \dots, a_j\}$. Для каждой пары (c_j, a_j) определяется вектор откликов $y_{ij} \in R^K$ по K экономическим и поведенческим критериям. Требуется построить политику персонализации $\pi: C \rightarrow A$, максимизирующую векторный функционал $F(\pi) = (F_1(\pi), F_2(\pi), \dots, F_K(\pi))$ при заданных бюджетных и операционных ограничениях вида $\sum_i c(a_{\pi(i)}) \leq B$. Поскольку критерии содержательно противоречат друг другу (например, рост маржи и снижение оттока), решение задачи ищется в смысле Парето-оптимальности: формируется фронт недоминируемых политик, среди которых лицо, принимающее решение, выбирает компромиссную точку, соответствующую стратегии бизнеса. Математически поиск недоминируемых политик сводится к нахождению такого подмножества решений, при котором невозможно улучшить значение одного критерия без ухудшения хотя бы одного другого. Это требует перехода от скалярных функций потерь к многомерной оптимизационной среде.

Архитектура системы. Предлагаемая интеллектуальная система имеет модульную структуру и включает четыре основных компонента: (1) подсистему предобработки данных и сегментации клиентов, (2) ансамбль моделей глубокого обучения для прогнозирования отклика клиента на предложения, (3) ядро многокритериальной оптимизации, (4) подсистему оценки качества и обратной связи. Общая структурная схема системы представлена на рисунке 1.

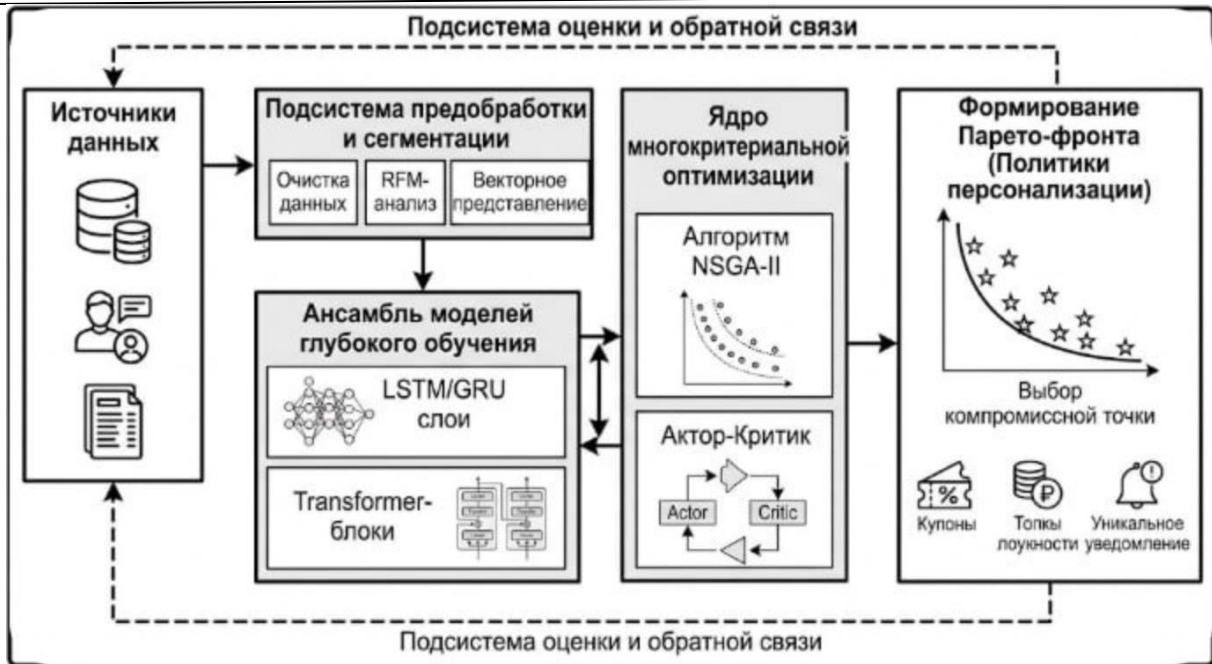


Рисунок 1. Структурная схема интеллектуальной системы многокритериальной оптимизации программы лояльности

Для прогнозирования поведения клиентов используется гибридная нейросетевая архитектура, объединяющая рекуррентные слои (LSTM/GRU) для обработки последовательности транзакций и блоки внимания (Transformer-блоки) для учёта долгосрочных зависимостей. Включение механизма самовнимания позволяет модели фокусироваться на недавних аномальных всплесках активности клиента, игнорируя при этом рутинные транзакции, не несущие предиктивной ценности. Входной тензор формируется из истории покупок, демографических признаков, активности в каналах коммуникации и реакции на предшествующие предложения. На выходе модель оценивает вероятностные характеристики отклика клиента по каждому из K критериев. Параметры θ модели обучаются минимизацией составной функции потерь $L(\theta) = \sum_K \lambda_K * L_K(\theta)$, где L_K — потери, соответствующие k -му целевому критерию, а коэффициенты λ балансируют их вклад.

Ядро многокритериальной оптимизации реализовано на основе модифицированного эволюционного алгоритма NSGA-II с интеграцией методов обучения с подкреплением по схеме «актор-критик». В данной архитектуре нейросетевой прогноз отклика играет роль внутреннего симулятора (модели среды), что позволяет проводить большое число виртуальных взаимодействий без затрат на реальные маркетинговые кампании. Агент обучается в виртуальной среде, где награда формируется на основе векторного функционала отклика. Применение NSGA-II обеспечивает получение равномерно распределённого Парето-фронта, а включение схемы «актор-критик» повышает скорость сходимости в пространстве политик персонализации высокой размерности. Подсистема обратной связи накапливает фактический отклик клиентов и периодически дообучает модели прогноза, поддерживая устойчивую точность при изменении поведения аудитории и появлении новых маркетинговых акций.

Результаты экспериментального исследования. Для апробации разработана программная реализация системы на языке Python с использованием библиотек PyTorch, NumPy и DEAP. Эксперименты проводились на синтетическом наборе данных, моделирующем поведение 100 000 клиентов в течение 12 месяцев, и на анонимизированных данных программы лояльности торговой сети. В качестве базовых моделей сравнения использовались случайная политика, политика «единое предложение для всех», классическая сегментация по RFM-признакам и градиентный бустинг с одной целевой функцией (прибыль). Оценка проводилась по четырём критериям: ожидаемая прибыль на клиента, удельная выручка, индекс удовлетворённости (NPS-прокси) и прогнозируемая вероятность удержания. Обобщённые результаты приведены в таблице 1.

Таблица 1.

Сравнение качества базовых моделей и предложенной системы

Модель	Прибыль, %	NPS-прокси, %	Удержание, %
Единое предложение	100	100	100
RFM-сегментация	104	102	103

Градиентный бустинг	108	101	104
Предложенная система	114	107	108

Полученные результаты показывают, что предложенная интеллектуальная система обеспечивает прирост удельной выручки на 12–18 % по сравнению с базовыми моделями при одновременном повышении прогнозируемого индекса удовлетворённости клиента на 6–9 %. Примечательно, что градиентный бустинг, оптимизированный исключительно под прибыль, показал стагнацию индекса удовлетворённости, что в долгосрочной перспективе неизбежно ведёт к росту оттока. Эволюционный алгоритм NSGA-II с поддержкой нейросетевого прогноза формирует более широкий и равномерный Парето-фронт, что предоставляет лицу, принимающему решение, возможность выбора компромиссной точки в зависимости от текущих приоритетов бизнеса — максимизации краткосрочной прибыли или долгосрочного удержания клиентов.

Заключение. В работе предложена архитектура интеллектуальной системы многокритериальной оптимизации программ лояльности на основе моделей глубокого обучения. Совместное применение гибридной нейросетевой модели прогнозирования, методов обучения с подкреплением и эволюционного алгоритма NSGA-II позволяет получать набор Парето-оптимальных политик персонализации и существенно повышать экономическую эффективность программы лояльности при соблюдении операционных ограничений. Дальнейшие исследования связаны с интеграцией методов онлайн-обучения с подкреплением, разработкой интерпретируемых моделей принятия решений и распространением подхода на омниканальные программы лояльности с учётом каузальных эффектов маркетинговых воздействий.

Литература

1. Goodfellow I., Bengio Y., Courville A. Deep Learning. — Cambridge: MIT Press, 2016. — 800 p. Sutton R.S., Barto A.G. Reinforcement Learning: An Introduction. 2nd ed. — Cambridge: MIT Press, 2018. — 552 p.
2. Deb K. Multi-objective Optimization Using Evolutionary Algorithms. — Chichester: Wiley, 2001. — 497 p.
3. Hochreiter S., Schmidhuber J. Long Short-Term Memory // Neural Computation. — 1997. — Vol. 9, № 8. — P. 1735–1780.
4. Vaswani A. et al. Attention Is All You Need // Advances in Neural Information Processing Systems. — 2017. — Vol. 30. — P. 5998–6008.
5. Чабаненко Д.Н., Кузнецов А.А. Программы лояльности в розничной торговле: модели и алгоритмы // Прикладная информатика. — 2021. — Т. 16, № 4. — С. 35–48.
6. Воронцов К.В. Машинное обучение: курс лекций. — М.: МФТИ, 2020. — 220 с.

DEVELOPMENT OF AN INTELLIGENT MULTI-CRITERIA OPTIMIZATION SYSTEM FOR LOYALTY PROGRAMS BASED ON DEEP LEARNING MODELS

postgrad. Yarovoy A.A.

Financial University under the Government of Russian Federation

The paper presents the concept of an intelligent system for multi-criteria optimization of loyalty programs based on deep learning models. Loyalty programs are a key customer retention tool in retail, banking and telecommunications; however, their efficiency is limited by the complexity of balancing conflicting criteria such as campaign profitability, customer satisfaction, purchase frequency and churn probability. The proposed system combines recurrent neural networks (LSTM/GRU) with attention-based blocks for customer behavior forecasting, reinforcement learning for personalized offer generation and the NSGA-II evolutionary algorithm for Pareto-optimal search. The architecture includes a customer segmentation module, a response prediction module, a multi-criteria optimization core and a feedback subsystem. Experimental validation on synthetic and anonymized retail data has shown an increase in predicted unit revenue by 12–18 % and an improvement of the customer satisfaction index by 6–9 % compared to baseline models.



АЛГОРИТМ ПОИСКА И КОРРЕКЦИИ ОШИБОК В МОДУЛЯРНОМ КОДЕ НА ОСНОВЕ РАСШИРЕНИЯ СИСТЕМЫ ОСНОВАНИЙ

асп., Гапочкин А.В.

Московский политехнический университет

В работе рассмотрены вопросы поиска и коррекции ошибок при помощи системы остаточных классов (СОК). Одним из наиболее важных применений системы остаточных классов является контроль ошибок в числах, передаваемых по каналам связи. В статье описывается алгоритм исправления ошибок, основанных на расширении системы оснований. Этот способ характеризуется модульностью составляющих его операций и эффективностью по сравнению с существующими традиционными аналогами.

Операции, выполняемые над данными, представленными в системе остаточных классов (СОК), можно разделить на два вида: модульные и немодульные. Модульные операции характеризуются тем, что при их выполнении не происходит переносов данных между разрядами. Это позволяет осуществлять такие операции параллельно относительно каждого разряда, что увеличивает быстродействие всего алгоритма в целом. Немодульные операции, в свою очередь, носят позиционный характер, однако без них не может обойтись практически любой алгоритм в СОК. Сложность выполнения немодульных операций ограничивает возможности СОК в обработке информации. В частности, в области коррекции ошибок [1,4].

В качестве основного недостатка каждого модулярного кода выступает его свойство – непозиционность. Другими словами, используя систему остаточных классов нельзя определить его местоположения относительно рабочего диапазона. Поэтому при разработке алгоритмов поиска и исправления ошибок в кодах системы остаточных классов используют позиционные характеристики [2].

Однако осуществлять процедуры поиска и коррекции ошибок можно с использованием алгоритмов расширения системы оснований модулярного кода. Как правило, такие процедуры сводятся к вычислению по значениям остатков рабочих оснований остатков по контрольным основаниям. В данной работе будет рассмотрен алгоритм обнаружения и исправления ошибок, который использует эту процедуру.

Как и ранее, рассмотрим систему остаточных классов с двумя контрольными основаниями, которые удовлетворяют условию (1). В этом случае берется исходная непозиционная комбинация числа $A = (\alpha_1, \dots, \alpha_k, \alpha_{k+1}, \alpha_{k+2})$, а затем на основе k информационных остатков $\alpha_1, \alpha_2, \dots, \alpha_k$, производят вычисления остатков по контрольным основаниям $\alpha'_{k+1}, \alpha'_{k+2}$. Затем происходит вычисление синдрома ошибки по этим двум контрольным основаниям согласно

$$\begin{cases} \delta_{k+1} = |\alpha'_{k+1} - \alpha_{k+1}|_{p_{k+1}}^+ \\ \delta_{k+2} = |\alpha'_{k+2} - \alpha_{k+2}|_{p_{k+2}}^+ \end{cases} \quad (1)$$

Очевидно, что если синдром ошибки равен нулю, то это свидетельствует о том, что исходный код СОК не содержит ошибку. Если вычисленные значения остатков по контрольным основаниям $\alpha'_{k+1}, \alpha'_{k+2}$ не совпадет с исходными величинами остатков избыточных оснований α_{k+1} и α_{k+2} , то это свидетельствует о том, что модулярная комбинация СОК является запрещенной. При этом по величине синдрома ошибки можно однозначно определить ошибочное основание, а также величину ошибки [3,5].

Пусть зада упорядоченная система остаточных классов, которая содержит k рабочих оснований $p_1, p_2, \dots, p_k$ и два контрольных модуля p_{k+1}, p_{k+2} , удовлетворяющих условию (1). В этом случае код СОК числа $A = (\alpha_1, \alpha_2, \dots, \alpha_{k+2})$ не содержит ошибок, если выполняется условие

$$|\alpha_j - \alpha'_j|_{p_j}^+ = 0, \quad (2)$$

где $\alpha'_j = \left| C_j |p_j - \sum_{i=1}^k \alpha_i K_i + R_a|_{p_j}^+ \right|_{p_j}^+$; $C_j = |K_j^{-1}|_{p_j}^+$; R_a – ранг числа A в безизбыточной СОК; $K_i = [B_i / P_{\text{раб}}]$; $j=k+1, k+2$.

При разработке данного алгоритма использовалась позиционная характеристика – интервальный номер числа, представленного в коде СОК [4]. Известно, что интервальный номер l , в котором находится код СОК числа A вычисляется

$$l_{\text{инт}} = [A / P_{\text{раб}}]. \quad (3)$$

Используя китайскую теорему об остатках, можно провести преобразование из модулярного кода в позиционный код числа согласно

$$A = \sum_{i=1}^{k+3} \alpha_i B_i \bmod P_{\text{полн}}. \quad (4)$$

Подставив последнее равенство в выражение (3) и, воспользовавшись свойством сравнимости ортогональных базисов полной и безизбыточной системы остаточных классов, получаем

$$l_{\text{инт}} = \left| \sum_{i=1}^{k+2} \alpha_i K_i + R_a \right|_{P_{\text{раб}}}^+ \Big|_{P_{\text{конт}}}^+, \quad (5)$$

где $K_i = [B_i/P_{\text{раб}}]$; $R_a = [\sum_{i=1}^k \alpha_i B_i^*/P_{\text{раб}}]$; $B_i^* \equiv B_i \bmod P_{\text{раб}}$; $P_{\text{конт}} = \prod_{i=k+1}^{k+2} p_i$.

Произведем замену величины

$$P_{\text{конт}} = \prod_{i=k+1}^{k+2} p_i = p_j$$

Тогда равенство (5) примет вид

$$l_{\text{инт}} = \left| \sum_{i=1}^k \alpha_i K_i + r_a + R_j \alpha'_j \right|_{p_j}^+ \quad (6)$$

Известно, что код СОК числа удовлетворяет условию $A < P_{\text{раб}}$, то интервальный номер будет равен нулю $l = 0$. Следовательно, справедливо

$$\left| K_j \alpha'_j \right|_{p_j}^+ = \left| \sum_{i=1}^k \alpha_i K_i + R_a \right|_{P_{\text{раб}}}^+ \Big|_{p_j}^+ \quad (7)$$

Тогда

$$\alpha'_j = \left| C_j \left| p_j - \sum_{i=1}^k \alpha_i K_i + R_a \right|_{P_{\text{раб}}}^+ \right|_{p_j}^+, \quad (8)$$

где $C_j = \left| K_j^{-1} \right|_{p_j(z)}^+$.

Таким образом, на основании (8) было произведено вычисление остатков α'_j по контрольным основаниям на основе известных значений $\alpha_1, \alpha_2, \dots, \alpha_k$.

Следовательно, если выполняется условие

$$\left| \alpha_j - \alpha'_j \right|_{p_j}^+ = 0,$$

то комбинация $A = (\alpha_1, \alpha_2, \dots, \alpha_{k+2})$ не содержит ошибки [6].

Рассмотрим пример использования данного алгоритма расширения оснований [2]. Пусть имеется упорядоченная система остаточных классов, имеющая рабочие основания $p_1=2, p_2=3, p_3=5$. В этом случае, рабочий диапазон будет равен $P_{\text{раб}} = 30$. Контрольными основаниями в данной системе остаточных классов выберем модули $p_4=7$ и $p_5=11$. В результате этого полный диапазон такой системы равен $P_{\text{полн}} = 2310$.

Проведем вычисление ортогональных базисов избыточной СОК. Тогда ортогональные базисы равны

$$B_1 = m_1 p_2 p_3 p_4 p_5 = 1155$$

$$B_2 = m_2 p_1 p_3 p_4 p_5 = 1540$$

$$B_3 = m_3 p_1 p_2 p_4 p_5 = 1386$$

$$B_4 = m_4 p_1 p_2 p_3 p_5 = 330$$

$$B_5 = m_5 p_1 p_2 p_3 p_4 = 210$$

Чтобы осуществить реализацию алгоритма, представим ортогональные базисы в следующем виде

$$B_1 = 1155 = K_1 P_{\text{раб}} + B_1^* = 38 \cdot 30 + 15$$

$$B_2 = 1540 = K_2 P_{\text{раб}} + B_2^* = 51 \cdot 30 + 10$$

$$B_3 = 1386 = K_3 P_{\text{раб}} + B_3^* = 46 \cdot 30 + 6$$

$$B_4 = 330 = K_4 P_{\text{раб}} = 11 \cdot 30$$

$$B_5 = 210 = K_5 P_{\text{раб}} = 7 \cdot 30$$

Вычислим значения частных K_i по модулю $p_4 = 7$. В результате получаем следующие значения

$$\left| K_1 \right|_{p_4}^+ = \left| 38 \right|_7^+ = 3$$

$$\left| K_2 \right|_{p_4}^+ = \left| 51 \right|_7^+ = 2$$

$$\left| K_3 \right|_{p_4}^+ = \left| 46 \right|_7^+ = 4$$

$$\left| K_4 \right|_{p_4}^+ = \left| 11 \right|_7^+ = 4$$

Произведем вычисление следующего сомножителя выражения (8). В результате получаем

$$C_4 = |K_4^{-1}|_{p_4}^+ = |4^{-1}|_7^+ = 2.$$

Вычислим значения частных K_i по второму контрольному модулю $p_5 = 11$. В результате получаем следующие значения

$$\begin{aligned} |K_1|_{p_5}^+ &= |38|_{11}^+ = 5 \\ |K_2|_{p_5}^+ &= |51|_{11}^+ = 7 \\ |K_3|_{p_5}^+ &= |46|_{11}^+ = 2 \\ |K_5|_{p_5}^+ &= |7|_7^+ = 7 \end{aligned}$$

Произведем вычисление следующего сомножителя выражения (8). В результате получаем

$$C_5 = |K_5^{-1}|_{p_5}^+ = |7^{-1}|_{11}^+ = 8.$$

В качестве примера возьмем код числа $A=(0,2,2,2,2) = 2$. Проведем вычисление значений остатков по контрольным основаниям для данного числа, применяя разработанный алгоритм.

Вычислим значение ранг в без избыточной системы, определяемые основаниями $p_1=2, p_2=3, p_3=5$.

$$R^* = \left[\sum_{j=1}^k \alpha_j B_j^* / P_{\text{раб}} \right] = \left[\frac{0 \cdot 15 + 2 \cdot 10 + 2 \cdot 6}{30} \right] = 1$$

В этом случае получаем, что вычисленное значение первого остатка по контрольному основанию $p_4 = 7$ для данной комбинации согласно (8) равно

$$\begin{aligned} \alpha'_4 &= \left| C_4 \right|_{p_4} - \left| \sum_{i=1}^3 \alpha_i K_i + R_a \right|_{p_4}^+ \left| \right|_{p_4}^+ = |2|_7 - |3 \cdot 0 + 2 \cdot 2 + 4 \cdot 2 + 1|_7^+ |_7^+ = \\ &= |2|_7 - 6|_7^+ |_7^+ = 2 \end{aligned}$$

Произведем вычисление значения второго контрольного вычета по модулю $p_5 = 11$. Тогда

$$\begin{aligned} \alpha'_5 &= \left| C_5 \right|_{p_5} - \left| \sum_{i=1}^3 \alpha_i K_i + R_a \right|_{p_5}^+ \left| \right|_{p_5}^+ = |8|_{11} - |5 \cdot 0 + 7 \cdot 2 + 2 \cdot 2 + 1|_{11}^+ |_{11}^+ = \\ &= |8|_{11} - 8|_{11}^+ |_{11}^+ = 2 \end{aligned}$$

Воспользуемся выражением для определения синдрома ошибки (1). В этом случае получаем

$$\begin{cases} \delta_4 = |\alpha'_4 - \alpha_4|_{p_4}^+ = |2 - 2|_{p_4}^+ = 0 \\ \delta_5 = |\alpha'_5 - \alpha_5|_{p_5}^+ = |2 - 2|_{p_5}^+ = 0 \end{cases}$$

Так как в результате вычисления синдрома ошибки был получен нулевой результат, то для данного случая является истинным утверждение - проверяемая комбинация СОК

$A = (0,2,2,2,2)$ не содержит ошибки.

Таким образом, использование непозиционных кодов СОК позволяет не только повышать скорость и точность проводимых вычислений за счет использования малоразрядных и целых остатков, но и обеспечивает коррекцию ошибочных кодовых комбинаций. Для этого в состав оснований СОК вводят дополнительные избыточные основания. Для проведения поиска и коррекции ошибок необходимо использовать позиционные характеристики, которые показывают расположение числа A , представленного в модулярном коде, относительно рабочего диапазона.

Литература

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 с.
2. Барбарян В.Г., Гапочкин А.В., Калмыков М.И., Мартыросян А.Г. Применение операции расширения системы оснований модулярного кода для обнаружения и коррекции ошибки // Успехи современного естествознания. 2014. № 11-2. С. 56-58.
3. Червяков Н.И., Сахнюк П.А., Шапошников А.В., Макоха А.Н. Нейрокомпьютеры в остаточных классах. – М.: «Радиотехника», 2003. – 272 с.

4. Червяков Н.И., Авербух В.М., Бабенко М.Г., Ляхов П.А., Гладков А.В., Гапочкин А.В. Приближенный метод выполнения немодульных операций в системе остаточных классов // Фундаментальные исследования. 2012. № 6-1. С. 189-193.
5. Червяков Н.И., Шапошников А.В., Ряднов С.А. Модулярные параллельные вычислительные структуры нейропроцессорных систем. – М.: Физматлит, 2002. – 288 с.
6. Чипига А.Ф., Калмыков И.А. Структура нейронной сети для реализации цифровой обработки сигналов повышенной разрядности// Наука. Инновации. Технологии. - 2004. - Т.38.- С. 46.

ALGORITHM FOR SEARCHING AND CORRECTING ERRORS IN MODULAR CODE BASED ON THE EXPANSION OF THE BASIS SYSTEM

graduate Gapochkin A.V.

Moscow Polytechnic University

The paper discusses the search and correction of errors using the residual class system (RCS). One of the most important applications of the residual class system is the control of errors in numbers transmitted over communication channels. The article describes an algorithm for correcting errors based on the expansion of the base system. This method is characterized by the modularity of its constituent operations and its efficiency compared to existing traditional methods.



СЕКЦИЯ № 5.

РАДИОСВЯЗЬ

ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ СИСТЕМЫ МУЛЬТИПЛЕКСИРОВАНИЯ С ОРТОГОНАЛЬНЫМ ЧАСТОТНЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ ЗА СЧЕТ СНИЖЕНИЯ ОТНОШЕНИЯ ПИКОВОЙ МОЩНОСТИ К СРЕДНЕЙ С ПОМОЩЬЮ ЦИКЛИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ СДВИГА В ЧАСТОТНОЙ ОБЛАСТИ (FDCSS)

соискатель Волошин Е.А., д.т.н., проф. Калмыков И.А.,

Северо-Кавказский федеральный университет

. При ортогональном мультиплексировании с частотным разделением каналов (OFDM) возникает проблема, известная как отношение пиковой мощности к средней (PAPR). Выбранное отображение (SLM) и ограничение являются эффективными методами снижения PAPR. Следовательно, в этой статье для уменьшения PAPR предлагается схема, основанная на циклической последовательности сдвига в частотной области (FDCSS), в сочетании с SLM и методом отсечения. Тщательный выбор значений сдвига, уровня ограничения и последовательности фаз снижает PAPR и улучшает производительность системы OFDM. Результаты этой новой схемы проверяются с помощью моделирования в среде Matlab при различных последовательностях фаз, поднесущих и значениях сдвига.

Метод мультиплексирования с ортогональным частотным разделением каналов (OFDM) – наиболее перспективный и эффективный метод мультиплексирования, который позволяет достичь высокой скорости передачи данных благодаря особой характеристике, известной как ортогональность поднесущих [1]. Благодаря этому он был внедрен в ряд систем связи, таких как беспроводные локальные сети (WLAN), цифровое аудиовещание (DAB), цифровое видеовещание (DVB) и т.д. Помимо всех этих преимуществ, у OFDM есть существенный недостаток – проблема пиковой амплитудно-частотной характеристики, которая снижает производительность системы. Поэтому крайне желательно снизить пиковую амплитудно-частотную характеристику с помощью эффективного алгоритма.

Схема с циклическим сдвигом (CSS), представленная Kee-Hoon Kim [2], которая улучшает производительность системы OFDM за счет уменьшения PAPR за счет циклического сдвига сигналов OFDM и добавления последовательности с частичным циклическим сдвигом и, наконец, выбора последовательности, которая генерирует минимальный PAPR.

Джун-Янг и др. [3] предложили методику в котором была представлена схема SLM класса III, в которой для генерации сигнала OFDM во временной области использовалось только одно обратное быстрое преобразование Фурье (IFFT), и подчеркивалось, что необходимо случайным образом выбирать значения циклического сдвига. На рис.4, 5 показан циклический сдвиг и инверсия во времени для сигнала OFDM с частичной переданной последовательностью (partial transmitted sequence – PTS) для уменьшения PAPR.

Методы кодирования [6] также используются для сокращения PAPR, но их большая таблица поиска требует огромного объема памяти. Другой важный метод, позволяющий избежать искажений, называется частичной переданной последовательностью (PTS) [7]. В этом методе последовательность в частотной области делится на несколько частичных последовательностей после преобразования во временной области с использованием обратного быстрого преобразования Фурье (IFFT). Затем эти последовательности суммируются, и для передачи выбирается последовательность, обеспечивающая минимальный пик-фактор. Кроме того, наиболее важным методом снижения пик-фактора без искажений является метод выборочного отображения (SLM) [8], в котором используются различные фазовые последовательности в частотной области. Эти фазовые последовательности умножаются на последовательность данных, после чего происходит преобразование во временную область с помощью обратного быстрого преобразования Фурье. Для передачи выбирается последовательность, обеспечивающая минимальный пик-фактор. Для снижения пикового отношения амплитуды к длительности используется метод клиппирования [9], который обрезает последовательность, генерирующую очень высокую мгновенную мощность, с помощью определенного порогового значения.

OFDM, PAPR и CCDF

В OFDM последовательность в частотной области [6] $X(k)$, прошедшая обратное быстрое преобразование Фурье (ОБПФ), преобразуется в соответствующую последовательность во временной области $x(n)$ следующим образом:

$$x(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X(k) e^{\frac{j(2\pi nk)}{N}} \quad n \in [0, N-1], \quad (1)$$

где N , n и k – количество поднесущих, индексы времени и частоты соответственно.

В системе OFDM все поднесущие ортогональны друг другу, и эта ортогональность между поднесущими создается вышеупомянутым уравнением IFFT (1).

Отношение пиковой мощности к средней объясняется как отношение пиковой мощности к средней мощности сигнала во временной области, генерируемого IFFT, и представлено следующим образом [6],

$$PAPR(x[n]) = \frac{\max(|x[n]|^2)}{E[x[n]^2]}. \quad (2)$$

Приведенное выше уравнение применимо после генерации сигнала во временной области из уравнения (1) для вычисления PAPR из уравнения (2) таким образом, чтобы соответствующий необходимо принять меры для того, чтобы уменьшить эту проблему.

Дополнительная функция кумулятивного распределения (CCDF) объясняется как вероятность того, что PAPR последовательности во временной области окажется больше определенного порогового значения b ,

$$CCDF(PAPR(x[n])) = \Pr(PAPR(x[n]) > PAPR0), \quad (3)$$

где Pr – вероятность; $PAPR0$ – заданный порог.

После расчета PAPR OFDM-сигнала во временной области по формуле (2) необходимо провести статистический анализ обычного OFDM-сигнала во временной области или OFDM-системы на основе предложенного алгоритма, чтобы оценить и сравнить эффективность обычной OFDM-системы и OFDM-системы на основе предложенного алгоритма.

Информация в частотной области определяется следующим образом, $X = [X(0), X(1), X(2), X(N-1)]$, которая генерируется из источника и передается через 8-PSK модулятор, а модулированные данные представляются в виде X_m , где N – количество используемые поднесущие представлены в виде,

$$X_m = [X_m(0), X_m(1), X_m(2) \dots X_m(N-1)]. \quad (4)$$

Модулированные данные X_m , передаваемые через блок FDCSS и блок циклического сдвига вправо, приводят к генерации q различных строк данных с циклическим сдвигом вправо, представленных в виде X^s .

$$X^s = \begin{bmatrix} X^1(0) & X^1(1) & X^1(2) \dots & X^1(N-1) \\ X^2(0) & X^2(1) & X^2(2) \dots & X^2(N-1) \\ X^3(0) & X^3(1) & X^3(2) \dots & X^3(N-1) \\ \dots & \dots & \dots & \dots \\ X^q(0) & X^q(1) & X^q(2) \dots & X^q(N-1) \end{bmatrix}, \quad (5)$$

где $1 < s < q$.

Для оптимизации используется последовательность фаз, определенная ниже, $P^v = [P^v(0), P^v(1), P^v(2) \dots P^v(N-1)] \in \{-1, +1, -j, +j\}$ (где $1 < v < U$) – это используется для элементарного умножения в частотной области с последовательностью данных, генерируемой с помощью результатов блока FDCSS,

$$X^v = [X^s(0) * P^v(0) \dots X^s(N-1) * P^v(N-1)]. \quad (6)$$

Теперь рассмотрим значения $v = 1$ и s от 1 до 5, которые дают следующий результат:

$$X^1 = \begin{bmatrix} X^1(0) * P^1(0) & \dots & X^1(N-1) * P^1(N-1) \\ X^2(0) * P^1(0) & \dots & X^2(N-1) * P^1(N-1) \\ X^3(0) * P^1(0) & \dots & X^3(N-1) * P^1(N-1) \\ X^4(0) * P^1(0) & \dots & X^4(N-1) * P^1(N-1) \\ X^5(0) * P^1(0) & \dots & X^5(N-1) * P^1(N-1) \end{bmatrix}. \quad (7)$$

После определения последовательности в частотной области и применения уравнения IFFT (1) для генерации сигнала во временной области в дальнейшем, PAPR для вышеуказанной последовательности, сгенерированной во временной области, представленной x_v , вычисляется по уравнению (2) и сохраняется минимальная последовательность PAPR после U -кратного повторения, которая показана в виде,

$$x = [x^1, x^2, x^3, x^4, \dots x^q], \quad (8)$$

где $1 < s < q$.

Если последовательность во временной области генерирует очень высокие значения PAPR, применяется обрезка с использованием определенного порогового значения,

$$x_{clip}(n) = \begin{cases} B; & |x(n)| > B \\ X(n); & |x(n)| \leq B \end{cases}, \quad (9)$$

где $x(n)$ – сигнал во временной области, B – уровень клиппирования, $x_{clip}(n)$ – сигнал с клиппированием.

Наконец, сохраняются все последовательности FDCSS от 1 до q , и в итоге для передачи выбирается последовательность, обеспечивающая минимальный пик-фактор.

$$x = [x_{clip}^1, x_{clip}^2, x_{clip}^3, x_{clip}^4, \dots, x_{clip}^q]. \quad (10)$$

Для предложенной последовательности циклических сдвигов в частотной области было проведено моделирование в Matlab на основе выбранного отображения в сочетании с методом ограничения, где поднесущие $N = 32, 64$ и 128 ; последовательности фаз равной 6 и 11; порог ограничения равным 0.85, метод цифровой модуляции используется 8-PSK, использовалась повышающая выборка равная 4, OFDM-блоки по 5000, круговой сдвиг вправо на 20.

На рисунке 1 показаны результаты моделирования при $CCDF=10^{-3}$. Уровни PAPR (дБ) для исходной системы OFDM, SLM, клиппирования и FDCSS-SLM-клиппирования при $N = 32$, количестве фазовых последовательностей 6, уровне клиппирования 0.85 и правом циклическом сдвиге 20 составляют 9.55, 8.35, 9.1 и 7 дБ соответственно. Таким образом, можно сделать вывод, что максимальное снижение PAPR достигается за счет предложенного метода FDCSS-SLM-clipping.

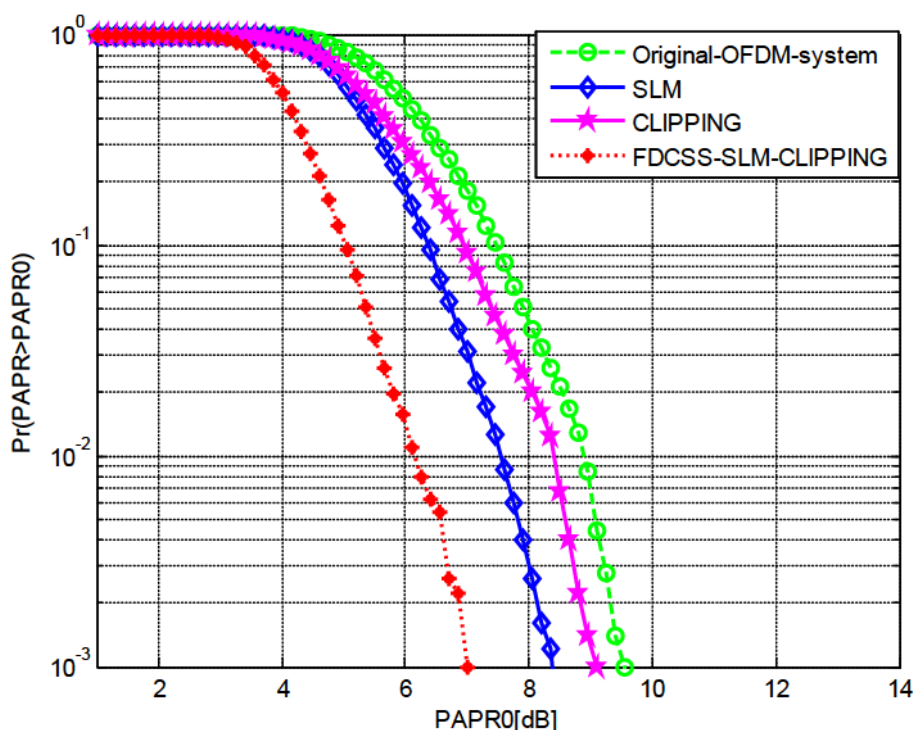


Рисунок 1 – Сравнительный анализ исходной системы OFDM, SLM, клиппирования и FDCSS-SLM-clipping

На рисунке 2 показаны результаты моделирования при $CCDF = 0,001$. На графике представлены уровни PAPR (дБ) для исходной системы OFDM, SLM, клиппирования и FDCSS-SLM-клиппирования при $N = 64$, количестве фазовых последовательностей 6, уровне клиппирования 0.85 и правом круговом сдвиге 20 составляют 10.75, 9.10, 10.15 и 7.9 соответственно. Таким образом, можно сделать вывод, что максимальное снижение PAPR достигается за счет предложенной системы FDCSS-SLM-clipping.

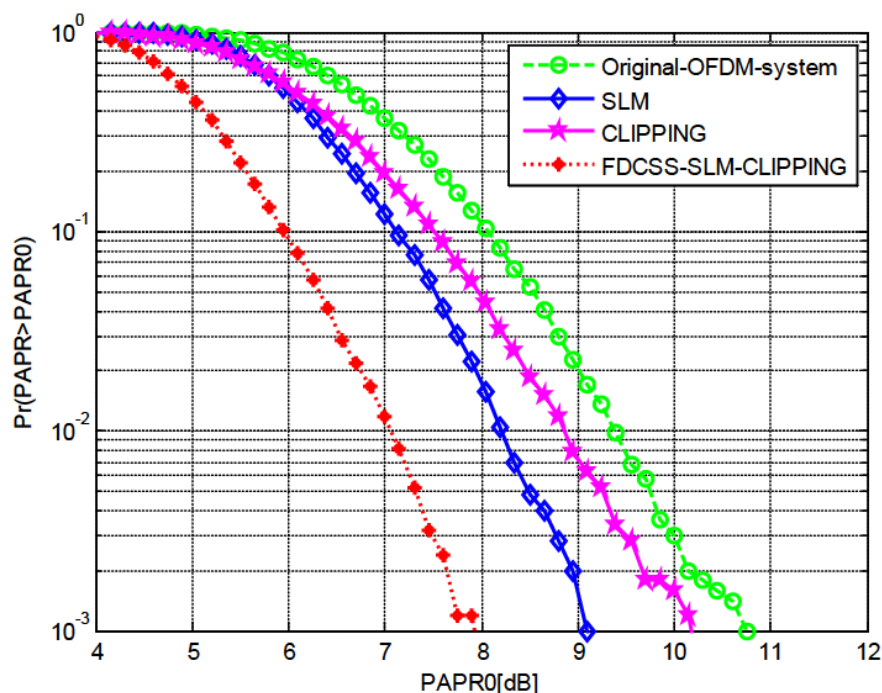


Рисунок 2 – Сравнительный анализ исходной системы OFDM, SLM, клиппирования и FDCSS-SLM-clipping

На рисунке 3 показаны результаты моделирования при CCDF = 0,001. Уровни PAPR (дБ) для исходной системы OFDM, SLM, клиппирования и FDCSS-SLM-клиппирования при $N = 128$, количестве фазовых последовательностей 6, уровне клиппирования 0.85 и правом циклическом сдвиге 20 составляют 10.60, 9.55, 10.0 и 8.5 соответственно. Таким образом, можно сделать вывод, что максимальное снижение PAPR достигается за счет предложенной системы FDCSS-SLM-clipping.

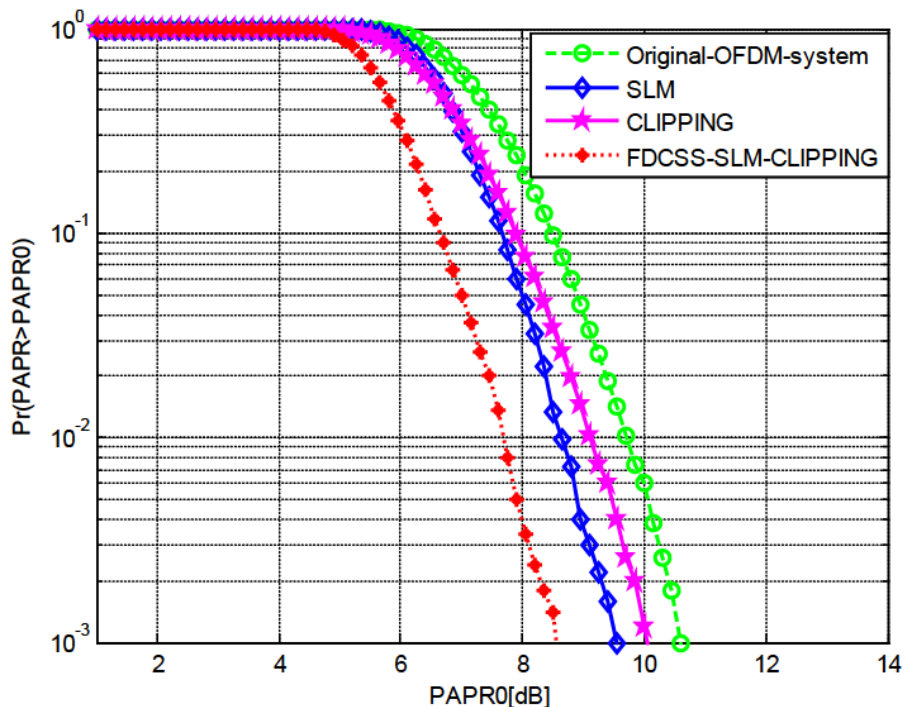


Рисунок 3 – Сравнительный анализ исходной системы OFDM, SLM, клиппирования и FDCSS-SLM-clipping

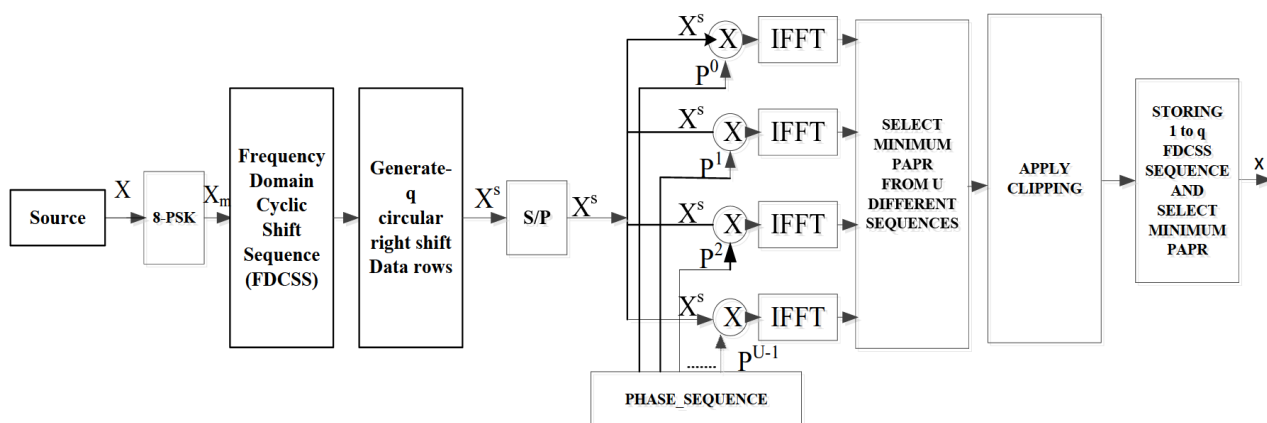


Рисунок 4 – Структурная схема предлагаемой последовательности циклических сдвигов в частотной области (FDCSS) в сочетании с методами селективного отображения (SLM) и клиппирования

На рисунке 5 показаны результаты моделирования при CCDF = 0,001. Уровни PAPR (дБ) для исходной системы OFDM, SLM, клиппирования и FDCSS-SLM-клиппирования при $N = 32$, количестве фазовых последовательностей 11, уровне клиппирования 0.85 и правом циклическом сдвиге 20 составляют 10, 7.3, 9.55 и 5.6 дБ соответственно. Таким образом, можно сделать вывод, что максимальное снижение пикового значения отношения сигнал/шум достигается за счет предложенного метода FDCSS-SLM-clipping

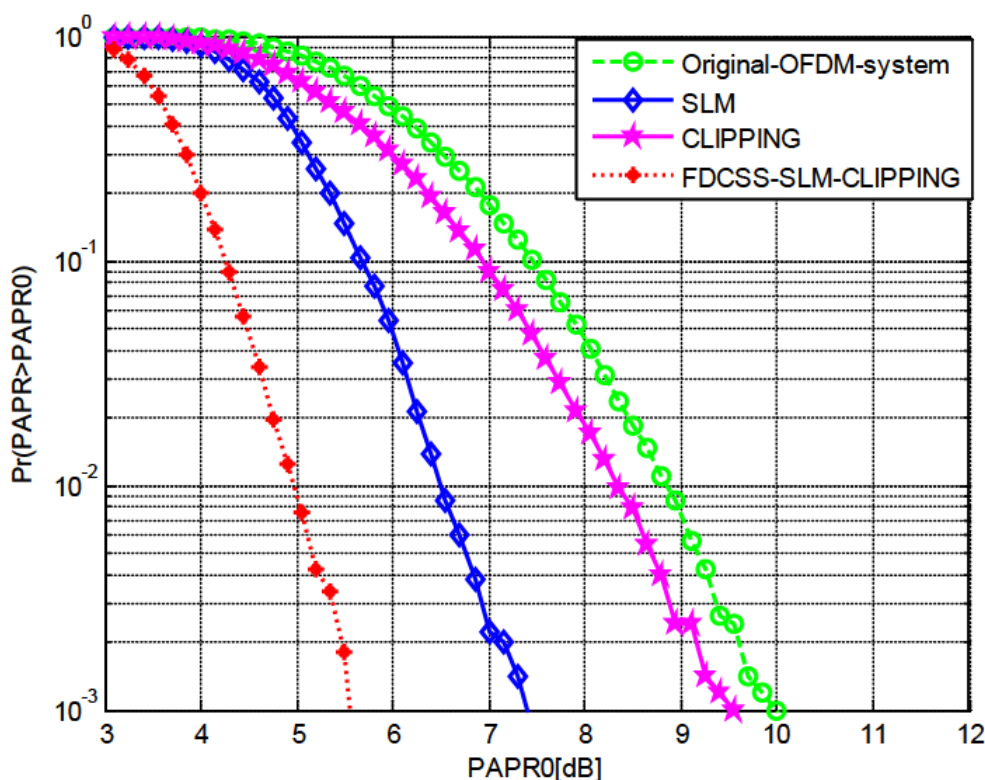


Рисунок 5 – Сравнительный анализ исходной системы OFDM, SLM, клиппинга и FDCSS-SLM-clipping

На рисунке 6 представлены результаты моделирования при CCDF = 0,001. Показаны уровни PAPR (дБ) для исходной системы OFDM, SLM, с клиппированием и FDCSS-SLM-с клиппированием при $N = 64$, количестве фазовых последовательностей 11, уровне клиппирования 0.85 и правом циклическом сдвиге 20. Значения составляют 10.15, 8.05, 9.7 и 6.55 соответственно. Таким образом, можно сделать вывод, что максимальное снижение PAPR достигается за счет предложенной схемы FDCSS-SLM-clipping.

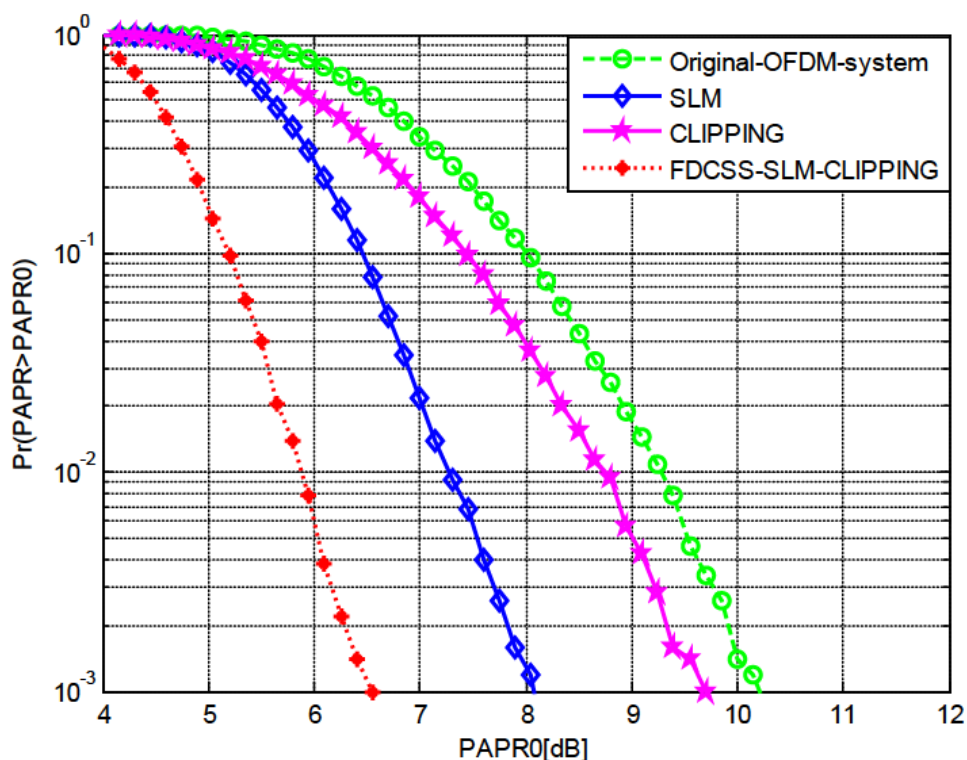


Рисунок 6 – Сравнительный анализ исходной системы OFDM, SLM, клиппирования и FDCSS-SLM-clipping

На рисунке 7 показаны результаты моделирования при CCDF = 0,001. Уровни PAPR (дБ) для исходной системы OFDM, SLM, клиппирования и FDCSS-SLM-клиппирования при $N = 128$, количестве фазовых последовательностей 11, уровне клиппирования 0.85 и правом циклическом сдвиге 20 составляют 11.05, 8.25, 10.45 и 7.01 дБ соответственно. Таким образом, можно сделать вывод, что максимальное снижение PAPR достигается за счет предложенного метода FDCSS-SLM-clipping.

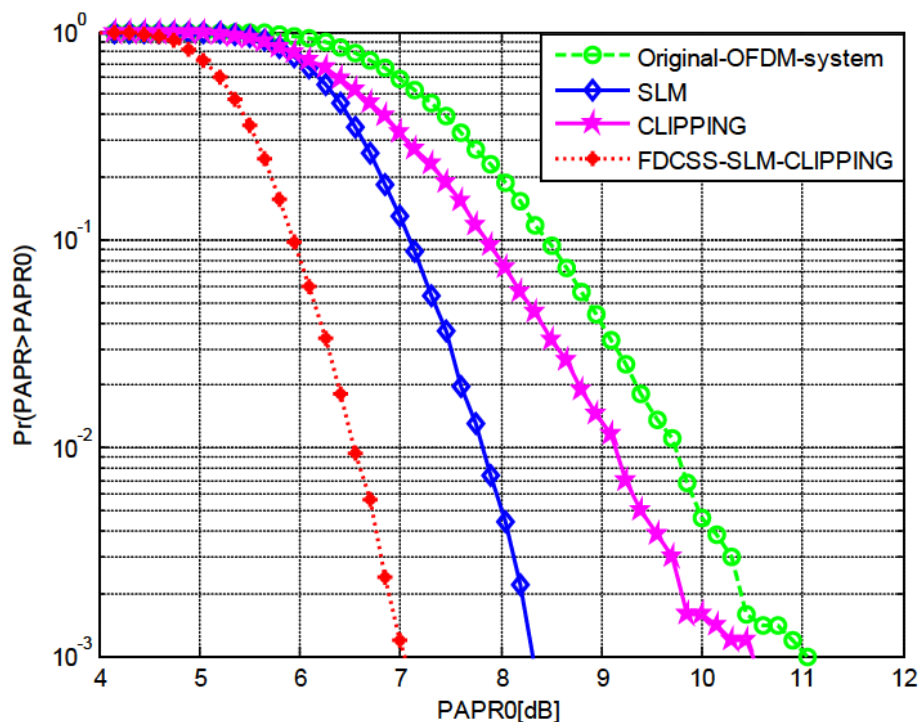


Рисунок 7 – Сравнительный анализ исходной системы OFDM, SLM, клиппирования и FDCSS-SLM-clipping

В этой статье предлагается использовать выбранное отображение на основе последовательности циклических сдвигов в частотной области (Frequency domain cyclic shift sequence, FDCSS) в сочетании с методом клиппирования для снижения пиковой амплитудно-частотной характеристики (PAPR) OFDM. Было использовано общее количество фаз 6 и 11 с 32, 64 и 128 поднесущими и 20 правыми циклическими сдвигами. Каждый результат моделирования наглядно демонстрирует высокую эффективность предложенного алгоритма. Во всех вышеупомянутых случаях достигается значительный выигрыш, что подтверждается соответствующими результатами моделирования CCDF. Таким образом, предложенный алгоритм гораздо эффективнее снижает PAPR по сравнению с исходными алгоритмами OFDM, SLM и клиппированием.

Литература

1. Tao Jiang, Yiyang Wu. An overview Peak-to-Average Power Ratio Reduction Techniques for OFDM Signals, Broadcasting. IEEE Trans, 2008 June; 54:257-68.
2. Kee-Hoon Kim. On the Shift value Set of Cyclic Shifted Sequence for PAPR Reduction in OFDM Systems. IEEE Transactions on Broadcasting. 2016; 62:496-500.
3. Woo Jun-Young, Joo Hyun Seung, Kim Kee-Hoon, No Jong-Seon, Shin Dong-Joon. PAPR Analysis of Class-III SLM Scheme Based on Variance of Correlation of Alternative OFDM Signal Sequences. IEEE Communication Letters. 2015; 19:989-92.
4. Hill G, Faulkner M, Singh J. Cyclic shifting and time inversion of partial transmit sequence to reduce the peak to average power ratio in OFDM. 2000; 2:1256-59.
5. Hill G, Faulkner M, Singh. Reducing the peak to average power ratio in OFDM by cyclically shifting partial transmitted sequence. 2000; 36:561-61.
6. Gupta P, Kumar BA, Jain SK. Peak to average power ratio reduction in OFDM using higher order partitioned PTS sequence and Bose Chaudhuri Hocquenghem Codes. Proc. IEEE Conf. SPACES-2015. 2015 Jan; p. 443-447
7. Gupta P, Kumar, Arun Kumar B, Jain SK, Singh B. An Improved and Efficient PAPR Reduction Method in OFDM System Using Modified Partial Transmitted Sequence. Proc. Conf. EBAS-2014. 2014 Nov; p. 261-64.
8. Lingyin Wang, Ju Liu. Partial phase weighting selected mapping scheme for peak-to-average power ratio reduction in orthogonal frequency division multiplexing system. IET Communications. 2015 Jan; 9(2):147-55.
9. Deepa T, Swetha K, Kumar R. A joint clipping and logarithmic based companding for the reduction of peak-to-average power ratio in OFDM system. Proc. IEEE Conf. ICICES-2013. 2013 Feb; p. 655-59.

PERFORMANCE IMPROVEMENT OF ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING SYSTEM BY REDUCING PEAK TO AVERAGE POWER RATIO USING FDCSS (FREQUENCY DOMAIN CYCLIC SHIFT SEQUENCE) COMBINED WITH SLM AND CLIPPING TECHNIQUE

prof. Kalmykov I.A., asp. E.A. Voloshin

North Caucasus Federal University

Abstract: Orthogonal frequency division multiplexing (OFDM) undergoes a problem known as peak to average power ratio (PAPR). Selected mapping (SLM) and clipping are the efficient techniques to diminish the PAPR. Hence, in this paper, a frequency domain cyclic shift sequence (FDCSS) based scheme combined with SLM and clipping technique is proposed for the reduction of PAPR. Careful selection of the shifting values, clipping level, and phase sequence reduces PAPR and improves the performance OFDM system. The results of this novel scheme are validated through Matlab simulations under various phase sequences, sub-carriers and shifting values.



ОЦЕНКА ПОЛОСЫ ПРОПУСКАНИЯ СПУТНИКОВОГО РАДИОКАНАЛА ПО РЕЗУЛЬТАТАМ ГНСС-МОНИТОРИНГА ИОНОСФЕРЫ

проф. Пашинцев В. П., асп. Гринев Е. М., асп. Диптан П. А.

Северо-Кавказский федеральный университет

Разработан аппаратно-программный комплекс оценки полосы дисперсионных искажений и полосы когерентности замираний в спутниковом (трансионосферном) канале связи на основе результатов зондирования ионосферы с помощью глобальных навигационных спутниковых систем (ГНСС). С этой целью решены следующие задачи: 1) разработки комплексной модели изменения полного электронного содержания в ионосфере с мелкомасштабными неоднородностями; 2) разработки структурно-физической модели трансионосферного канала связи с дисперсионными искажениями и замираниями различных типов; 3) оценки полос дисперсионности и когерентности трансионосферного радиоканала при различных состояниях ионосферы; 4) разработка структуры построения аппаратно-программного комплекса оценки полосы когерентности и дисперсионности трансионосферного канала связи на основе результатов ГНСС-зондирования ионосферы.

Введение

Известно [1, 2], что при распространении широкополосных сигналов (ШПС) в системах спутниковой связи (ССС) через нормальную ионосферу (рис.1) могут возникать дисперсионные искажения (ДИ), которые вызывают энергетические потери при обработке сигналов ($\eta_d \leq 1$) и увеличивают вероятность их ошибочного приема $P_{\text{ош}} = \psi(h^2, \eta_d)$ при неизменном входном отношении h^2 сигнал/шум (С/Ш). Условием возникновения ДИ является превышение ширины спектра F_0 передаваемого сигнала над полосой дисперсионных искажений F_d трансионосферного канала: $F_0/F_d > 1$. Полоса ДИ зависит прямо пропорционально от несущей частоты f_0 сигнала и обратно пропорционально – от полного электронного содержания (ПЭС) ионосферы N_T на трассе распространения радиоволн (РРВ) [2]:

$$F_d = (y_0 c f_0^3 / 80, 8 \pi N_T)^{1/2}, \quad (1)$$

где коэффициент $y_0 = 0,35$ выбирается из соображений обеспечения потерь $\eta_d = 0,1$ дБ.

Недостаток оценки полосы ДИ согласно (1) состоит в том, что F_d должна определять величину η_d , а не зависеть от нее. Поэтому необходимо обосновать выражение для F_d , не зависящее от η_d , и определить зависимость $\eta_d = \psi(F_0/F_d) \leq 1$.

Следует отметить, что полоса пропускания трансионосферного канала определяется не только полосой ДИ (F_d), но и полосой когерентности (F_k) замираний, обусловленных рассеянием радиоволн на мелкомасштабных (10...1000 м) неоднородностях ионосферы при ее возмущениях (т.е. увеличении флуктуаций электронной концентрации (ЭК) ΔN_i относительно среднего значения ($\bar{N}$) ЭК). На рисунке 1 показан процесс рассеяния радиоволн на неоднородностях ЭК ионосферы и возникновения многолучевости в ССС при мелкомасштабных возмущениях ионосферы (ВИ).

Согласно рисунку 1 относительные фазовые $\Delta \varphi_i \propto \Delta N_i / f_0$ и временные $\Delta \tau_i \propto \Delta N_i / f_0^2$ запаздывания приходящих лучей возрастают при увеличении флуктуаций ЭК ионосферы ΔN_i и понижении несущей частоты f_0 сигнала ССС. При этом полоса когерентности замираний определяется как величина, обратная временным запаздываниям приходящих лучей [3]

$$F_k \approx 1/\Delta \tau_i. \quad (2)$$

В [4] установлена достаточно сложная аналитическая зависимость

$$P_{\text{ош}} = \psi(h^2, \eta_c, \eta_q) = \psi(h^2, F_0/F_k, 1/T_s F_k) \quad (3)$$

вероятности ошибки при некогерентном (НК) приеме в ССС сигналов с заданной шириной спектра F_0 и длительностью T_s от отношения С/Ш на входе приемника и коэффициентов энергетических потерь при

обработке сигналов с частотно-селективными замираниями (ЧСЗ) $\eta_{\text{ч}} = \psi(F_0/F_{\text{д}}) \leq 1$ и межсимвольной интерференцией (МСИ) $\eta_{\text{м}} = \psi(1/T_s F_{\text{к}}) \geq 0$.

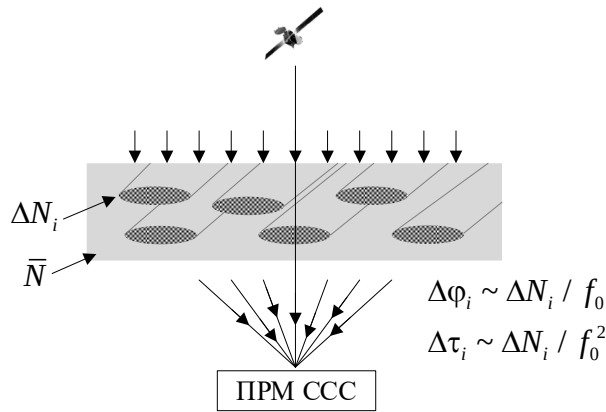


Рисунок 1 – Возникновение многолучевости в CCC при мелкомасштабных возмущениях ионосферы

При условии отсутствия ЧСЗ ($F_0/F_{\text{к}} \ll 1$), МСИ ($1/T_s F_{\text{к}} = \Delta\tau_i/T_s \ll 1$) выражение (3) сводится к известному [3] виду $P_{\text{ош}} = (h^2 + 2)^{-1}$ для оценки помехоустойчивости НК приема сигналов с неселективными релеевскими замираниями.

Проведенный выше анализ показал наличие следующих недостатков известных методов оценки полосы дисперсионных искажений (1) $F_{\text{д}} = \psi(N_T, f_0, y_0)$ и когерентности замираний (2) $F_{\text{к}} = \psi(\Delta N_i, f_0)$ в трансionoсферном канале:

1. Известные модели изменения ЭК в ионосфере учитывают или ПЭС ($N_T \square N(z_m)$) для оценки полосы дисперсионности $F_{\text{д}} = \psi(N_T, f_0, y_0)$, или флуктуации ЭК в мелкомасштабных неоднородностях ΔN_i для оценки полосы когерентности $F_{\text{к}} = \psi(\Delta N_i, f_0)$. Для одновременного учета фазовой дисперсии и дифракции (рассеяния) волны в ионосфере нужна комплексная ее модель, учитывающая мелкомасштабные флуктуации ЭК ионосферы ΔN_i относительно среднего значения $\bar{N}$.

2. Поскольку измерение на высоте максимума ионизации ионосферы ($z_m = 250...400$ км) средней ЭК $\bar{N}(z_m)$ и относительных флуктуаций $\Delta N_i(z_m)$ затруднено, то комплексная модель ионосферы должна учитывать среднее значение ПЭС $\bar{N}_T \square \bar{N}(z_m)$ ионосферы и мелкомасштабные флуктуации ПЭС $\Delta N_T \square \Delta N_i(z_m)$ на трассе РРВ, которые можно измерить наземным приемником ГЛОНАСС/GPS.

3. Характеристики замираний в спутниковом (трансionoсферном) КС с многолучевостью $F_{\text{к}} \approx 1/\Delta\tau_i$ определяются экспериментально и не учитывают их зависимости с от мелкомасштабных флуктуаций ПЭС ионосферы на трассе РРВ и выбора несущей частоты: $F_{\text{к}} = \psi(\Delta N_T, f_0)$.

4. Полоса ДИ трансionoсферного канала должна зависеть только от ПЭС ионосферы и несущей частоты сигнала $F_{\text{д}} = \psi(N_T, f_0)$ и не должна зависеть от типа приемника (определяющего коэффициент y_0 для обеспечения допустимых потерь при обработке сигналов $\eta_{\text{д}}$).

Цель доклада состоит в обосновании и разработке аппаратно-программного комплекса оценки полосы дисперсионных искажений и полосы когерентности замираний в спутниковом (трансionoсферном) канале связи на основе результатов зондирования ионосферы с помощью глобальных навигационных спутниковых систем (ГНСС). Для достижения этой цели необходимо решить следующие задачи: 1) обоснования комплексной модели изменения ПЭС в ионосфере с мелкомасштабными неоднородностями; 2) разработки структурно-физической модели трансionoсферного канала связи с дисперсионными искажениями и замираниями различных типов; 3) оценки полос дисперсионности и когерентности трансionoсферного радиоканала при различных состояниях ионосферы; 4) разработка структуры построения аппаратно-

программного комплекса оценки полосы когерентности и дисперсионности трансionoсферного канала на основе результатов ГНСС-зондирования ионосферы.

Комплексная модель изменения пэс в ионосфере с мелкомасштабными неоднородностями

Известно [5], что распределение ЭК в слоях ионосферы с мелкомасштабными неоднородностями (рисунок 2) описывается совокупностью изменения по высоте z ее среднего значения $\bar{N}(z)$ и пространственных ($\rho = x, y$) флуктуаций $\Delta N(\rho, z)$:

$$N(\rho, z) = \bar{N}(z) + \Delta N(\rho, z). \quad (4)$$

На рисунке 2 приведено распределение (4) по высоте ЭК ионосферы с мелкомасштабными неоднородностями (а) и комплексная модель ПЭС ионосферы в виде совокупности толстого однородного слоя с максимальной средней ЭК $\bar{N}_m$ эквивалентной толщиной z_3 и тонкого слоя неоднородностей (б).

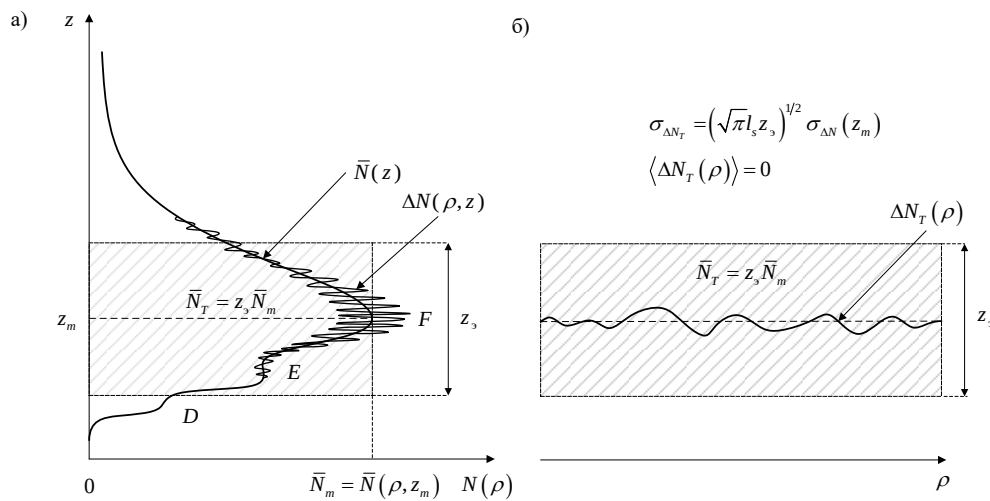


Рисунок 2 – Распределение по высоте электронной концентрации ионосферы с мелкомасштабными неоднородностями (а) и комплексная модель ПЭС ионосферы (б)

Связь между распределением ЭК ионосферы и ее ПЭС описывается выражением [4, 5]

$$N_T(\rho) = \int_{z_u} N(\rho, z) dz = \int_{z_u} (\bar{N}(z) + \Delta N(\rho, z)) dz = \bar{N}_T + \Delta N_T(\rho), \quad (5)$$

где среднее значение ПЭС $\bar{N}_T$ и мелкомасштабные флуктуации ПЭС $\Delta N_T(\rho)$ определяются как

$$\bar{N}_T = \int_{z_u} \bar{N}(z) dz = \int_0^{z_3} \bar{N}(z_m) dz = z_3 \bar{N}(z_m) = z_3 \bar{N}_m, \quad (6)$$

$$\Delta N_T(\rho) = \int_{z_u} \Delta N(\rho, z) dz. \quad (7)$$

Статистические характеристики пространственных флуктуаций ПЭС $\Delta N_T(\rho)$ характеризуются: 1) математическим ожиданием $\langle \Delta N_T(\rho) \rangle = 0$; 2) СКО флуктуаций ПЭС (при гауссовской корреляционной функции флуктуаций ЭК ионосферы) [4]

$$\sigma_{\Delta N_T} = \langle \Delta N_T(\rho)^2 \rangle^{0,5} = (\sqrt{\pi} l_s z_3)^{1/2} \sigma_{\Delta N}(z_m) = (\sqrt{\pi} l_s z_3)^{1/2} \beta_{\Delta N} \bar{N}_m. \quad (8)$$

где $\beta_{\Delta N}$ – интенсивность мелкомасштабных неоднородностей.

Структурно-физическая модель трансionoсферного канала с дисперсионными искажениями и замираниями

На рисунке 3 представлена структурно-физическая модель трансionoсферного канала, построенная на основе методов описания многолучевого РРВ (а) и дифракции (б) волны на неоднородностях ионосферы с учетом ее дисперсионных свойств [4, 6].

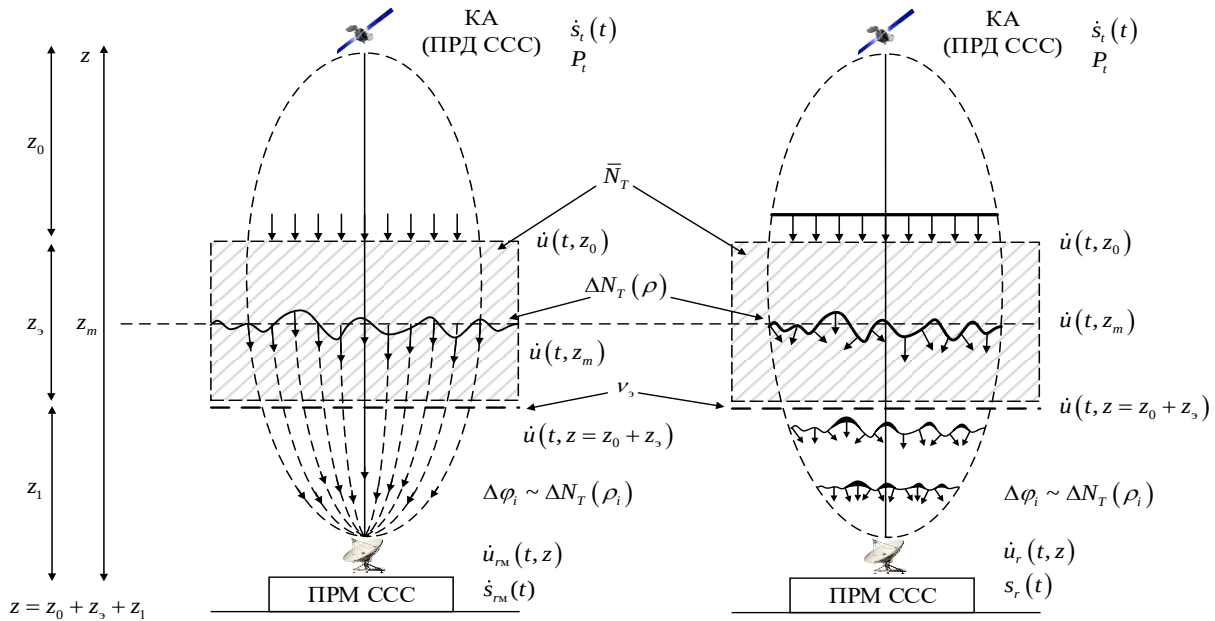


Рисунок 3

– Структурно-физическая модель трансionoсферного канала на основе описания многолучевости (а) и дифракции (б) волны в ионосфере с учетом ее дисперсионных свойств

При передаче комплексного сигнала $\dot{s}_t(t)$ фазовый фронт комплексной волны $\dot{u}(t, z_{0s})$ с частотой $\omega = \omega_0 + \Omega = 2\pi(f_0 + F)$ после прохождения тонкого неоднородного ионосферного слоя (фазового экрана) на выходе ионосферы описывается выражением:

$$\varphi(\rho, \omega, z_{0s}) = \bar{\varphi}(\omega, z_{0s}) + \Delta\varphi(\rho, \omega) + \Delta\Phi_d(\Omega), \quad (9)$$

где $\Delta\varphi(\rho, \omega)$ – флуктуации (искажения) фазового запаздывания во фронте выходной волны относительно среднего значения фазового запаздывания этой волны $\bar{\varphi}(\omega, z_{0s})$; $\Delta\Phi_d(\Omega)$ – нелинейный фазовый сдвиг волны по частоте $\omega = \omega_0 + \Omega$ по сравнению с ω_0 вследствие дисперсионности ионосферы.

Флуктуации фазового запаздывания во фронте выходной волны (9) прямо пропорционально зависят от флуктуаций ПЭС ионосферы $\Delta N_T(\rho)$:

$$\Delta\varphi(\rho, \omega) = \omega \Delta\tau_r(\rho) = (\omega_0 + \Omega) 40,4 \Delta N_T(\rho) / cf_0^2 = 80,8\pi(f_0 + F) \Delta N_T(\rho) / cf_0^2. \quad (10)$$

Дальнейший процесс РРВ в свободном пространстве до точки приема фазового экрана можно представить (рис. 3а) как результат суммирования множества лучей ($i=1 \dots M$), образуемых элементарными участками ρ_i на поверхности фазового фронта выходной волны с различными фазовыми сдвигами:

$$\begin{aligned} \Delta\varphi_i = \Delta\varphi(\rho_i, \omega) &= \omega \Delta\tau_r(\rho_i) = 2\pi(f_0 + F) 40,4 \Delta N_T(\rho_i) / cf_0^2 = \\ &= 80,8\pi \Delta N_T(\rho_i) / cf_0^2 + 80,8\pi F \Delta N_T(\rho_i) / cf_0^2. \end{aligned} \quad (11)$$

В качестве полосы когерентности F_k можно выбрать значение $|f - f_0| = F$, при котором последнее слагаемое (11) равно 1 радиан (т.е. $80,8\pi F \Delta N_T(\rho_i) / cf_0^2 = 1$ рад):

$$F_k = cf_0^2 / 80,8 \Delta N_T(\rho_i) = 1/2 \Delta\tau(\rho_i) \equiv 1/2 \Delta\tau_i. \quad (12)$$

В результате разработки структурно-физической модели трансionoсферного КС (рисунок 3) получены аналитические выражения для сигналов на входе ПРМ CCC с помощью методов построения многолучевых моделей КС $\dot{s}_{rm}(t)$ и с помощью радиофизического метода фазового экрана $\dot{s}_r(t)$. Анализ тождественности выражений для средней мощности этих сигналов позволяет оставить выражения для:

1) СКО флуктуаций фазового фронта волны (11) на несущей частоте $\omega_0 = 2\pi f_0$ на выходе ионосферы

$$\sigma_\varphi = \langle \Delta\varphi^2(\rho, \omega_0) \rangle^{0,5} = 80,8\pi\sigma_{\Delta N_T} / cf_0, \quad (13)$$

2) полосы когерентности трансionoсферного КС (которое соответствует по виду (12))

$$F_k = f_0 / \sigma_\varphi \sqrt{2 + d_1^2} = cf_0^2 / 80,8\pi\sigma_{\Delta N_T} \sqrt{2 + d_1^2}, \quad (14)$$

где $\sigma_{\Delta N_T} = \langle \Delta N_T(\rho)^2 \rangle^{0,5}$ – СКО флуктуаций ПЭС определяется согласно (8);

$$d_1^2 = 4(z_m)^2 c^2 / \pi^2 f_0^2 l_s^4, \quad (15)$$

– параметр, характеризующий нарастание дифракционных эффектов за фазовым экраном на высоте z_m ; l_s – характерный (средний) размер мелкомасштабных неоднородностей (10...1000 м). Последнее слагаемое в (9) описывается выражением [4]:

$$|\Delta\Phi_d(\Omega)| = 80,8\pi(f - f_0)^2 N_T(\rho) / cf_0^3, \quad (16)$$

где ПЭС ионосферы описывается выражением (5–7): $N_T(\rho) = \bar{N}_T + \Delta N_T(\rho)$.

В качестве полосы дисперсионных искажений F_d в трансionoсферном канале можно выбрать такое значение $|f - f_0| = F$, при котором $|\Delta\Phi_d(\Omega)| = 1$ радиан [7, 8]. Тогда получим:

$$F_d = (cf_0^3 / 80,8\pi N_T(\rho))^{1/2} = (cf_0^3 / 80,8\pi(\bar{N}_T + \Delta N_T(\rho)))^{1/2}. \quad (17)$$

С учетом соотношения $\bar{N}_T \gg \Delta N_T(\rho)$ выражение для полосы дисперсионных искажений в трансionoсферном канале можно записать как:

$$F_d = (cf_0^3 / 80,8\pi\bar{N}_T)^{1/2} = (cf_0^3 / 80,8\pi z_m \bar{N}_m)^{1/2}. \quad (18)$$

Таким образом, на основе структурно-физического подхода (комплексного применения методов построения многолучевых КС и радиофизического метода фазового экрана) получены искомые выражения (14, 15) и (18) для оценки зависимости полосы когерентности замираний $F_k = \psi(f_0, \sigma_{\Delta N_T})$ и дисперсионных искажений $F_d = \psi(f_0, \bar{N}_T)$ в трансionoсферном канале от выбора несущей частоты (f_0) и статистических характеристик ПЭС ионосферы ($\bar{N}_T, \sigma_{\Delta N_T}$) на трассе РРВ.

Оценка полос дисперсионности и когерентности трансionoсферного канала при различной ионосфере

Согласно [9], среднее значение и СКО мелкомасштабных флуктуаций ПЭС в нормальной среднеширотной ионосфере находятся в диапазоне значений $\bar{N}_T \approx 10^{17} \dots 10^{18} \text{ м}^{-2}$ и $\sigma_{\Delta N_T} \approx 10^{14} - 10^{15} \text{ м}^{-2}$, а в условиях естественных и искусственных возмущений ионосферы наибольшее среднее значение ПЭС не изменяется: $\bar{N}_T \approx 10^{18} \text{ м}^{-2}$, а диапазон СКО мелкомасштабных флуктуаций ПЭС может расширяться до значений $\sigma_{\Delta N_T} \approx 10^{16} - 10^{17} \text{ м}^{-2}$. В соответствии с этими исходными данными и полученными выражениями (14) и (18) на рис. 4 представлены зависимости полос когерентности (F_k) и дисперсионности (F_d) трансionoсферного КС от несущей частоты (f_0) и параметров ионосферы ($\bar{N}_T, \sigma_{\Delta N_T}$).

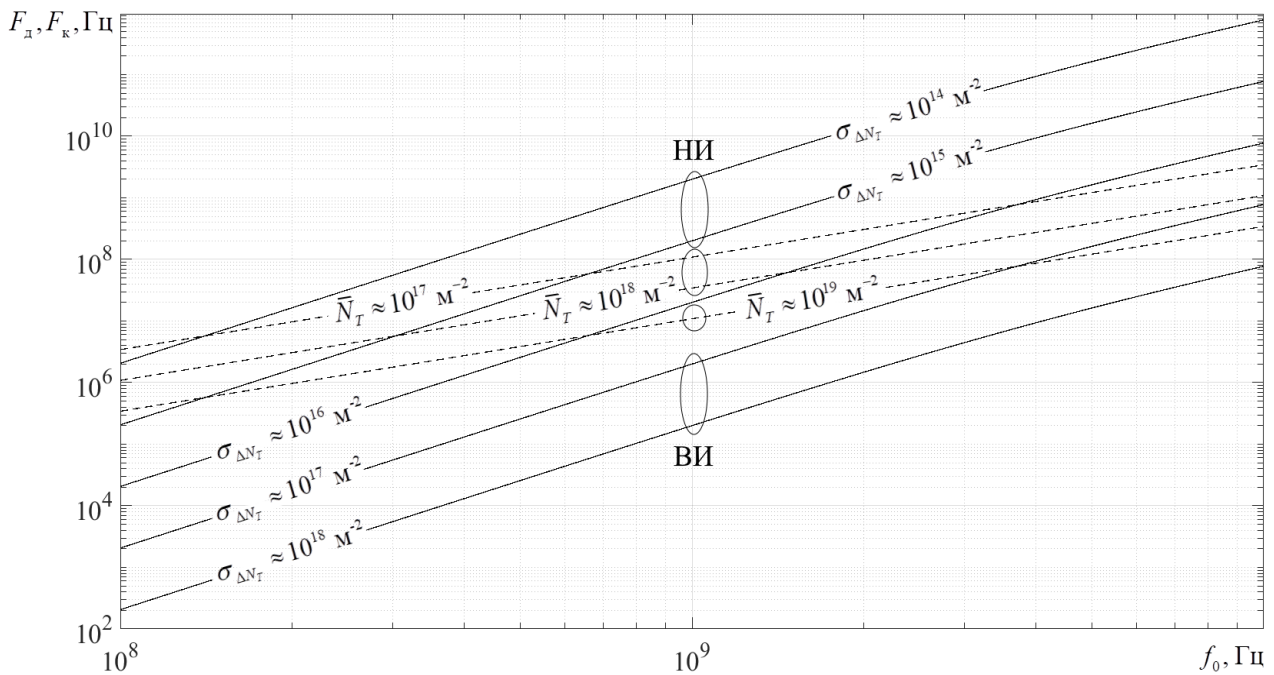


Рисунок 4 – Зависимости полос когерентности (F_k) и дисперсионности (F_d) трансionoсферного канала от несущей частоты (f_0) и параметров ионосферы ($\bar{N}_T$, $\sigma_{\Delta N_T}$)

Анализ содержания рисунка 4 показывает, что условиях нормальной ионосферы (НИ), когда $\bar{N}_T \approx 10^{17} \dots 10^{18} \text{ м}^{-2}$ и $\sigma_{\Delta N_T} \approx 10^{14} \dots 10^{15} \text{ м}^{-2}$, в диапазоне частот ССС $f_0 = 1 \dots 10 \text{ ГГц}$ при $l_s = 100 \text{ м}$ и $z_m = 300 \text{ км}$ полоса дисперсионных искажений трансionoсферного канала $F_d = 2 \cdot 10^7 \dots 3 \cdot 10^9 \text{ Гц} = 20 \text{ МГц} \dots 3 \text{ ГГц}$ на 1...2 порядка меньше полосы его когерентности $F_k = 2 \cdot 10^8 \dots 10^{12} \text{ Гц} = 200 \text{ МГц} \dots 10^3 \text{ ГГц}$. В условиях естественных и искусственных возмущений ионосферы (ВИ), когда $\bar{N}_T \approx 10^{19} \text{ м}^{-2}$, $\sigma_{\Delta N_T} \approx 10^{17} \dots 10^{18} \text{ м}^{-2}$, на несущей частоте $f_0 = 1 \text{ ГГц}$ полоса когерентности трансionoсферного канала составляет $F_k = 2 \cdot 10^5 \dots 2 \cdot 10^6 \text{ Гц} = 0,2 \dots 2 \text{ МГц}$, что меньше полосы дисперсионности в 5...50 раз ($F_d = 10^7 \text{ Гц} = 10 \text{ МГц}$). При повышении несущей до $f_0 = 10 \text{ ГГц}$ полосы дисперсионности и когерентности трансionoсферного канала увеличиваются на 1...2 порядка (до $F_d = 3 \cdot 10^8 \text{ Гц} = 300 \text{ МГц}$; $F_k \approx 10^8 \dots 10^9 \text{ Гц} = 0,1 \dots 1 \text{ ГГц}$).

Комплекс оценки полосы когерентности и дисперсионности трансionoсферного канала на основе гнсс-зондирования ионосферы

Известно [6], что двухчастотные (f_1 , f_2) приемники ГНСС типа GPS/ГЛОНАСС класса GISTM (GNSS Ionospheric and TEC Monitor) измеряют только среднего значения ПЭС ($\bar{N}_T$) на базе кодовых измерений (R'_1 , R'_2). Предложен способ модификации GISTM-приемника GPStation-6 для оценки полосы пропускания трансionoсферного канала (рисунок 5).

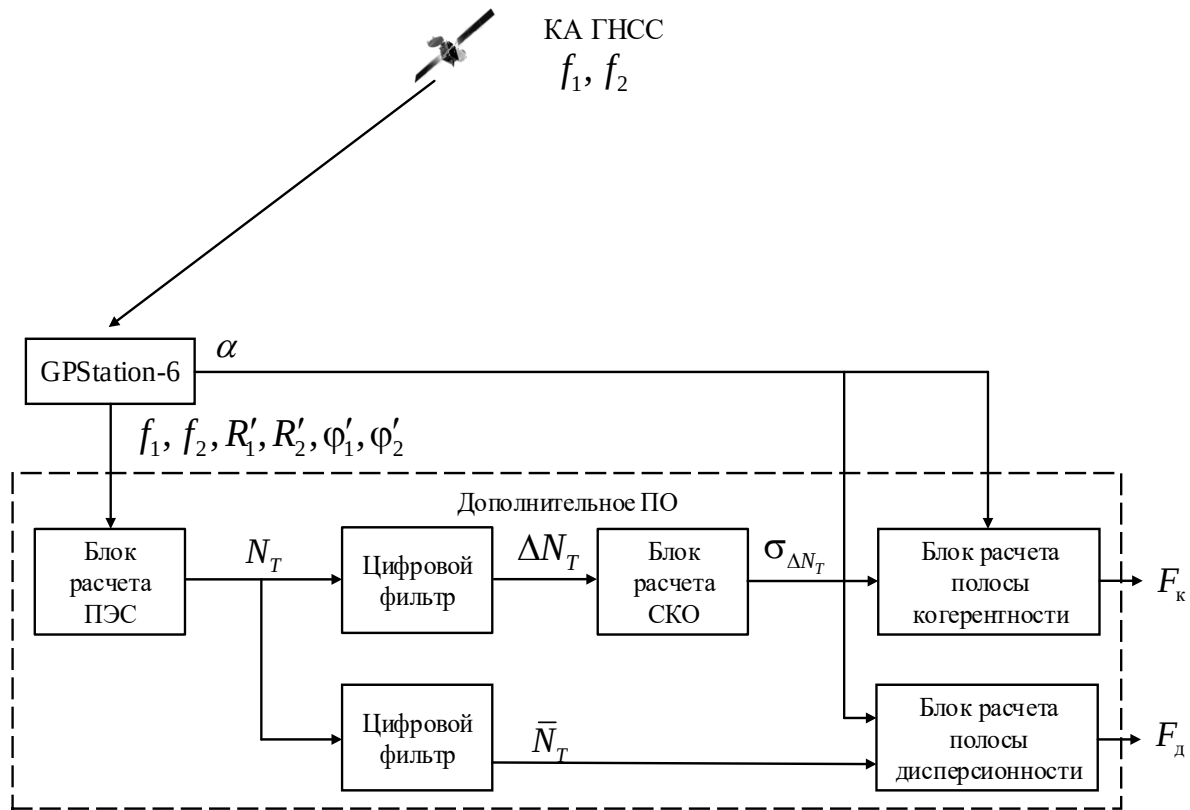


Рисунок 5 – Структурная схема программно-аппаратного комплекса оценки полосы пропускания трансionoсферного канала на основе ГНСС-зондирования ионосферы

Для этого в состав программного обеспечения GPStation-6 введены дополнительные блоки:

- 1) расчета ПЭС ионосферы (N_T) с уменьшенной шумовой погрешностью за счет комбинации кодовых (R'_1, R'_2) и фазовых (ϕ'_1, ϕ'_2) измерений;
- 2) цифровой фильтрации с частотой дискретизации 50 Гц для выделения среднего значения ПЭС ($\bar{N}_T$) и его мелкомасштабных флуктуаций (ΔN_T);
- 3) расчета СКО мелкомасштабных флуктуаций ПЭС ($\sigma_{\Delta N_T}$) ионосферы;
- 4) расчета полосы дисперсионных искажений трансionoсферного канала ($F_d \sim f_0^3 / \bar{N}_T$) в соответствии с выражением (18);
- 2) расчета полосы когерентности замираний трансionoсферного канала ($F_k \propto f_0^2 / \Delta N_T$) в соответствии с выражениями (8) и (14, 15).

Заключение

1. Разработана комплексная модель изменения полного электронного содержания в ионосфере с мелкомасштабными неоднородностями в виде (рис. 2) совокупности толстого однородного слоя, характеризуемого средним значением ПЭС (6), и тонкого слоя неоднородностей, характеризуемых СКО мелкомасштабных флуктуаций ПЭС (8).

2. Разработана структурно-физическая модель трансionoсферного канала с дисперсионными искажениями и замираниями различных типов на основе методов описания многолучевости и дифракции волны на неоднородностях ионосферы (рис. 3), которая позволяет получить искомые зависимости полосы дисперсионных искажений от среднего значения ПЭС в виде выражения (18) и полосы когерентности замираний от СКО мелкомасштабных флуктуаций ПЭС в виде выражения (14).

3. Произведена сравнительная оценка полос дисперсионности и когерентности трансionoсферного радиоканала (рис. 4) в диапазоне возможных изменений среднего значения ПЭС $\bar{N}_T \approx 10^{17} \dots 10^{19} \text{ м}^{-2}$ и СКО его мелкомасштабных флуктуаций $\sigma_{\Delta N_T} \approx 10^{14} \dots 10^{18} \text{ м}^{-2}$. Обосновано, что в традиционном диапазоне частот

ССС $f_0 = 1...10$ ГГц в условиях нормальной среднеширотной ионосферы полоса дисперсионности трансionoсферного канала на 1 – 2 порядка меньше полосы его когерентности. В условиях естественных и искусственных возмущений ионосферы на несущей частоте $f_0 = 1$ ГГц полоса когерентности трансionoсферного канала становится меньше полосы дисперсионности в 5...50 раз.

4. Разработана структура построения аппаратно-программного комплекса оценки полосы когерентности и дисперсионности трансionoсферного канала связи (рис. 5) на основе результатов ГНСС-зондирования ионосферы с помощью двухчастотного приемника GPStation-6 и модификации его программного обеспечения в направлении применения кодово-фазовых измерений и цифровой фильтрации результатов измерений с частотой дискретизации 50 Гц для выделения среднего значения ($\bar{N}_T$) и СКО мелкомасштабных флуктуаций ($\sigma_{\Delta N_T}$) ПЭС ионосферы.

Литература

1. Черенкова Л.Е., Чернышов О.В. Распространение радиоволн. – М.: Радио и связь, 1984. – 272 с.
2. Тепляков И.М. Ионосферные искажения цифровых сигналов с широкополосной модуляцией // Радиотехника. – 1984. – № 4. – С. 8–13.
3. Волков Л.Н., Немировский М.С., Шинаков Ю.С. Системы цифровой радиосвязи: базовые методы и характеристики. – М.: Эко Тренз, 2005. – 390 с.
4. Гундзе Е., Чжаохань Лю. Мерцания радиоволн в ионосфере // ТИИЭР. – 1982. – Т. 70. – № 4. – С. 5–45.
5. Пашинцев В.П. Модели трансionoсферных радиоканалов и помехоустойчивость систем космической связи. – Москва, Вологда: Инфра-Инженерия, 2026. – 212 с.
6. Пашинцев В.П., Песков М.В., Михайлов Д.А., Киселев Н.В. Оценка влияния дисперсионных и дифракционных свойств ионосферы на полосу пропускания трансionoсферного канала // Геомагнетизм и аэрономия. – 2024. – Т. 64. – С. 277 – 293.
7. Bedrosian E. Transionospheric propogation of FM signals // IEEE T. Commun. Techn. – 1970. – V. 18. – № 2. – P. 102–109.
8. Иванов Д.В., Иванов В.А., Рябова Н.В., Кислицын А.А. // Обеспечение предельной широкополосности систем спутниковой радиосвязи в условиях внутримодовой дисперсии трансionoсферных радиоканалов // Радиотехника и электроника. – 2023. – Т. 68. – С. 571– 578.
9. Рыжкина Т.Е., Федорова Л.В. Исследование статических и спектральных трансатмосферных радиосигналов УКВ-СВЧ диапазона // Журнал радиоэлектроники. – 2001. – № 2. <http://jre.cplire.ru/win/feb01/3/text.html>. 2001.

ESTIMATION OF THE SPECTRAL-COHERENT PARAMETERS OF THE SATELLITE COMMUNICATION CHANNEL BASED ON GPS MONITORING OF THE IONOSPHERE

Pashintsev P. V.¹, Grinev E. M.¹, Diptan P. A.¹

¹North-Caucasus Federal University

. A hardware and software complex has been developed for assessing the dispersion distortion band and coherence fading band in a satellite (trans-ionospheric) communication channel based on the results of ionosphere probing using global navigation satellite systems (GNSS). To achieve this goal, the following tasks were solved: 1) development of a comprehensive model for changing the total electron content in the ionosphere with small-scale inhomogeneities; 2) development of a structural and physical model for the trans-ionospheric communication channel with dispersion distortions and various types of fading; 3) assessment of the dispersion and coherence bands of the trans-ionospheric radio channel under different ionosphere conditions; 4) development of a structure for building a hardware and software complex for assessing the coherence and dispersion bands of the trans-ionospheric communication channel based on the results of ionosphere probing using GNSS.

Keywords: satellite communication systems, global navigation satellite systems, ionosphere, full electronic content, small-scale inhomogeneities, dispersion distortion band, coherence fading band.



О МЕТОДЕ ОЦЕНКИ УРОВНЯ СРЕДНЕЙ ЭНЕРГИИ ШУМА НА ОСНОВЕ АНАЛИЗА ПЛОТНОСТИ РАСПРЕДЕЛЕНИЯ ЭНЕРГИЙ В МОДЕМАХ ДИСКРЕТНЫХ ЧАСТОТНЫХ СИГНАЛОВ

асп. Иванов А.В.^{1,2}¹АО «Омский научно-исследовательский институт приборостроения»²Омский государственный технический университет

В работе рассматривается метод оценки среднего уровня энергии аддитивного белого гауссовского шума (далее АБГШ) для модемов дискретных частотных (далее ДЧ) сигналов. Новый метод основан на анализе плотности распределения энергий в ДЧ матрице. Проведён краткий обзор методов оценки энергии шума применимых для модемов ДЧ сигналов. Описаны основные этапы предлагаемого метода. Рассматривается вычислительная сложность алгоритмов, позволяющих реализовать новый метод. Проводится сравнение теоретической вычислительной эффективности нового метода и метода на основе порядковой статистики. Выдвигается теория о робастности нового метода и его самодостаточности для применения в модемах ДЧ сигналов, также рассматриваются случаи, когда применение нового метода ограничено.

В современных системах загоризонтной коротковолновой радиосвязи нашли применение модемы дискретных частотных (далее ДЧ) сигналов [1]. ДЧ сигналы являются результатом развития многопозиционной частотной телеграфии (далее МЧТ). Главным преимуществом модемов ДЧ сигналов перед модемами МЧТ является устойчивая работа в ионосферном радиоканале с замираниями.

При появлении первых модемов ДЧ сигналов возникла проблема, заключающаяся в отсутствии явного робастного метода демодуляции, позволяющего сделать выбор в пользу одной из гипотез из множества альтернатив. Главная особенность демодуляции ДЧ сигналов заключается в необходимости анализа данных в двумерном массиве – частотно-временной матрице (далее ДЧ матрице). Одним из первых применяемых методов демодуляции ДЧ сигналов, энергетическая эффективность которого приближалась к теоретической кривой, был метод приёма МЧТ расширенный для приёма ДЧ сигналов. Основная идея заключалась в применении подхода к демодуляции МЧТ по отдельности для каждой строки или столбца ДЧ матрицы. Рассмотренный метод демодуляции часто называют оптимальным [2]. Такой метод демодуляции устойчив к замираниям, однако плохо работал на практике при наличии сосредоточенных помех разного типа. Так наличие хотя бы одной мощной импульсной помехи приводило к практически полной неспособности демодулятора сделать выбор в пользу истинной гипотезы [3].

На смену данному методу демодуляции пришли первые методы косвенно использующие порядковую статистику [3-7]. Особенностью рассмотренных методов демодуляции является ранжирование энергий в слотах (ячейках) ДЧ матрицы и замене значения энергии на соответствующий энергии номер в одномерном массиве упорядоченному по возрастанию. Такой метод демодуляции часто называют ранговым. Главным преимуществом применения ранговых методов для демодуляции ДЧ сигнала стала устойчивая работа модема в условиях присутствия нескольких сосредоточенных помех различного типа [3, 8], однако ранговый метод демодуляции снизил энергетическую эффективность приёма в канале без сосредоточенных помех [3, 8]. Также одной из особенностей рангового метода демодуляции является отсутствие нормировки по строкам или столбцам.

Для дальнейшего улучшения энергетической эффективности модемов ДЧ сигналов и повышения их устойчивости к сосредоточенным помехам возникла необходимость отдельной оценки энергий для различных (несвязанных) процессов, влияющих на результирующую энергию в ДЧ матрице. Так перед принятием решения в пользу одной из гипотез необходимо провести отдельно оценку уровня средней энергии АБГШ по всей ДЧ матрице. Несмотря на множество возможных методов робастной оценки шума, большая часть из них основана на свойствах порядковой статистики [9-19]. Вероятно, на практике в большинстве случаев используется метод находящий перцентиль около 10% для массива энергий и умножающий его значение на корректирующий коэффициент который приблизительно равен 10. Следует уточнить, что данный метод работает только если массив энергий имеет экспоненциальное распределение – шум должен иметь нормальное распределение. Также амплитудно-частотная характеристика (АЧХ) принимающего устройства не должна иметь большую неравномерность в полосе пропускания. Неравномерность АЧХ может повлиять на оценку уровня средней энергии шума, что в некоторых случаях может быть существенным недостатком методов, основанных на порядковой статистике. Вычислительная сложность метода, основанного на порядковой статистике, линейно возрастает с увеличением количества слотов в ДЧ матрице, если для нахождения перцентилей используется алгоритм «Quickselect» (он же «Hoare's FIND») [20-22]. В случае если метод оценки будет использовать множество перцентилей вычислительная сложность может достигать линейно-логарифмической из-за использования алгоритмов быстрой

сортировки. Стоит уточнить, что алгоритм «Quickselect» имеет линейную сложность в среднем, однако может выполняться как быстрее, так и медленнее.

Метод оценки на основе порядковой статистике часто называется медианным. Такой метод получил широкое распространение и практически заменил другие методы оценки, став их логическим развитием. Так ранговый метод демодуляции также использует порядковую статистику, но не «извлекает» из метода статистического анализа полной эффективности. Это подводит к мысли, что использование методов статистического анализа не всегда приводит к полной утилизации их эффективной точности – методы постобработки могут иметь решающее значение в качестве (точности и разбросе) работы методов оценки.

Новый метод оценки уровня средней энергии шума

С увеличением размера ДЧ матрицы в современных модемах, а именно увеличением количества частотных подканалов и элементов сигнала, площадь ДЧ матрицы начинает включать достаточное количество слотов для прямого анализа плотности распределения энергий. Далее рассмотрим основные этапы нового метода.

Первый этап начинается после получения демодулятором ДЧ матрицы, состоящей из набора энергий. В случае если в слотах ДЧ матрицы содержатся результаты комплексной свёртки (комплексное число), необходимо перевести значения в слотах в энергию (сумма квадратов действительной и мнимой частей). После того как получена ДЧ матрица, содержащая энергии в слотах, необходимо перевести энергию в логарифмическую шкалу, например, дБ. Стоит уточнить, что формула перевод в дБ имеет дополнительный множитель перед логарифмом, для работы нового метода важна логарифмическая шкала, а не точное соответствие дБ – в случае ограниченных ресурсов множитель можно исключить из формулы. При возникновении проблем с производительностью также стоит рассмотреть использование функций для быстрого вычисления логарифмов, которые за счёт небольшого снижения точности позволяют получить ускорение в 5-10 раз в сравнении с стандартными функциями языка C++. Результатом работы первого этапа должна стать ДЧ матрица, заполненная энергией в логарифмическом масштабе.

Второй этап заключается в построении гистограммы плотности распределения для энергий в логарифмическом масштабе. Шаг между центрами столбцов (ширина столбцов) гистограммы зависит от количества слотов в ДЧ матрице, на момент написания работы точная формула расчёта неизвестна, шаг определяется эмпирически [8]. Также стоит обратить внимание на вычислительную сложность построения гистограммы плотности распределения. Существует как минимум два алгоритма построения гистограммы, один из алгоритмов является академическим – часто используется для объяснения методов статистического анализа имеет сложность схожую с квадратичной и прост для понимания. Второй алгоритм имеет линейную сложность и использует математические преобразования значений энергии напрямую в индекс столбца гистограммы, к которому принадлежит данное значение. Данный алгоритм построения гистограммы использовался в работе [8]. Результатом второго этапа должен являться одномерный массив содержащий гистограмму, отдельный элемент массива содержит количество слотов, энергия которых попадает в соответствующий индексу столбец гистограммы.

Третий этап – сглаживание результатов второго этапа. Необходимо провести сглаживание данных в гистограмме – провести фильтрацию фильтром скользящего среднего. Фильтр среднего можно оптимизировать за счёт хранения общей суммы и при прохождении данных на 1 отсчёт проводить одну операцию сложения с новым отсчётом и вычитания старого, выходящего из фильтра отсчёта, что может позволить достичь значительного ускорения в фильтрации.

Четвёртый этап – заключительный. Проводится поиск максимума в сглаженной гистограмме. Так как максимумом в гистограмме будет один из столбцов и индексы, соответствующие столбцам являются целочисленными, то такой подход не позволит получить точность оценки уровня средней энергии шума выше, чем разрешение гистограммы. Для устранения описанного недостатка необходимо перейти от целочисленных индексов к «виртуальным» индексам с плавающей точкой. Для осуществления подобного перехода необходимо провести интерполяцию по значениям максимума и соседним значениям с максимумом находящимся в гистограмме с целочисленными индексами. Интерполяция и нахождение максимума в интерполяционной кривой имеет единичную сложность, так как расчёты происходят по формулам. Первой формулой является выражения или их набор, позволяющий получить коэффициенты интерполяции для используемой интерполяционной функции. Для вычисления локального экстремума необходимо взять производную от функции интерполяции, приравнять её к нулю и решить полученное уравнение. Также следует учитывать, что вычисленный максимум в гистограмме – для энергий в логарифмической шкале, и для энергии АБГШ немного смещён в сторону на постоянную величину, после добавления смещений и масштабирования нового индекса с плавающей точкой результатом станет уровень средней энергии шума.

Суммарная вычислительная сложность нового метода может как незначительно превышать вычислительную сложность для методов на основе порядковой статистики, так и быть ниже, особенно при использовании реализаций на ПЛИС. Качество (точность, разброс результатов) работы нового метода зависит от выбранных параметров, в среднем, точность схожа с методом на основе порядковой статистики. Однако для большей информации необходимо проводить сравнение при различных состояниях радиоканала и для модемов ДЧ сигнала с ДЧ матрицами разного размера. Так для ДЧ матриц размером 7х7 метод на основе порядковой статистики может иметь большую точность, чем новый метод, однако при использовании матриц 37х37 результат может стать противоположным. При исследованиях, проводимых для работы [8] новый метод показал робастность и самодостаточность, что означает возможность использования нового метода без дополнительного ограничения с помощью метода на основе порядковой статистики, следовательно, ограничение, введенное в работе [8], является необязательным.

Одним из достоинств нового метода является расширение его возможностей до анализа среднего уровня энергий других, независимых от АБГШ, процессов в радиоканале, в том числе анализа энергий сосредоточенных помех и полезных сигналов, без затрат на вычислительные ресурсы на пересчет гистограммы. Гистограммы от разных ДЧ матриц можно как складывать (объединять), так и вычитать за линейное время, что открывает возможность для быстрого статистического анализа данных в области распределений на протяжении множества принятых ДЧ матриц.

Новый метод предлагается называть модальным, по аналогии с медианным методом, так как новый метод использует аналог моды, но для чисел с плавающей точкой. В дальнейшем планируется провести серию исследований для разработки алгоритма подбора параметров при проектировании модемов с использованием нового метода исходя из размера ДЧ матрицы. Также планируется провести серию исследований для получения зависимости качества оценок от выбранных параметров.

Литература

1. Варакин, Л. Е. Системы связи с шумоподобными сигналами. – Москва: Радио и связь, 1985. 384 с.
2. Будвис Н. С. Хмырова Н. П. Помехоустойчивость алгоритма демодуляции сигналов вида частотно-временных матриц // Успехи современной радиоэлектроники. 2013. № 10. С. 36–41.
3. Иванов А. В., Романов Ю. В. Помехоустойчивость рангового алгоритма демодуляции дискретных частотных сигналов в канале с АБГШ и сосредоточенными помехами // Техника радиосвязи. 2024. Выпуск 4 (63). С. 7–20.
4. Червяков В. Н. Ранговый алгоритм некогерентного обнаружения сигнала ЧВМ // Техника средств связи. Серия: Техника радиосвязи. 1985. Выпуск 10. С. 47–54.
5. Акимов П. С., Ефремов В. С. Ранговое обнаружение сигнала с большим динамическим диапазоном. - Радиотехника, 1978, т. 33, № 4, с. 66-69.
6. Акимов П. С., Кубасова А. Н. и Одинцова В. А. «Адаптивный ранговый обнаружитель» (1980 год, журнал «Радиотехника», том 35, №7, с. 50–53)
7. Акимов П. С., Ефремов В. С. Ранговая последовательная усеченная процедура многоканального обнаружения. - Радиотехника и электроника, 1976, т. 21, № 7, с. 1452-1457.
8. Ворошилов В. В., Иванов А. В., Романов Ю. В. Помехоустойчивость модифицированных алгоритмов демодуляции дискретных частотных сигналов в канале с АБГШ и сосредоточенными помехами // Техника радиосвязи. 2025. Выпуск 2 (65). С. 7–22.
9. Lloyd E. H. Least-squares estimation of location and scale parameters using order statistics //Biometrika. – 1952. – Т. 39. – №. 1/2. – С. 88-95.
10. Ogawa J. Determination of optimum spacings for the estimation of the scale parameter of an exponential distribution based on sample quantiles //Annals of the Institute of Statistical Mathematics. – 1960. – Т. 12. – С. 135-141.
11. Harter H. L. Estimating the parameters of negative exponential populations from one or two order statistics //The Annals of Mathematical Statistics. – 1961. – С. 1078–1090.
12. \David H. A., Nagaraja H. N. Order statistics. New York: John Wiley & Sons //David2Order Statistics1981. – 1981.
13. Finn H. M., Johnson R. S. Adaptive Detection Mode with Threshold Control as a Function of Spatially Sampled Clutter-Level Estimates // RCA Review. – 1968. – Vol. 29, № 3. – P. 414–463.
14. Rickard J. T., Dillard G. M. Adaptive detection algorithms for multiple-target situations // IEEE Transactions on Aerospace and Electronic Systems. – 1977. – Vol. AES-13, № 4. – P. 338–343.

15. Weiss, M. Analysis of some modified cell-averaging CFAR processors in multiple-target situations // IEEE Trans. Aerosp. Electron. Syst. – 1982. – Vol. AES-18, no. 1. – P. 102–114.
16. Rohling, H. Radar CFAR Thresholding in Clutter and Multiple Target Situations // IEEE Transactions on Aerospace and Electronic Systems. – 1983. – Vol. AES-19, iss. 4. – P. 608–621.
17. Gandhi P. P., Kassam S. A. Analysis of CFAR processors in nonhomogeneous background // IEEE Transactions on Aerospace and Electronic Systems. – 1988. – Vol. 24, № 4. – P. 427–445.
18. Ozgunes I., Gandhi P. P., Kassam S. A. A variably trimmed mean CFAR radar detector // IEEE Transactions on Aerospace and Electronic Systems. – 1992. – Vol. 28, № 4. – P. 1002–1014.
19. Himonas S. D., Barkat M. Automatic censored CFAR detection for nonhomogeneous environments // IEEE Transactions on Aerospace and Electronic Systems. – 1992. – Vol. 28, № 1. – P. 286–304.
20. Hoare C. A. R. Algorithm 63: Partition // Communications of the ACM. – 1961. – Vol. 4, № 7. – P. 321.
21. Hoare C. A. R. Algorithm 64: Quicksort // Communications of the ACM. – 1961. – Vol. 4, № 7. – P. 321.
- 22.** Hoare C. A. R. Algorithm 65: Find // Communications of the ACM. – 1961. – Vol. 4, № 7. – P. 321–322.

ON THE METHOD OF ESTIMATING THE LEVEL OF AVERAGE NOISE ENERGY BASED ON THE ANALYSIS OF THE ENERGY DISTRIBUTION DENSITY IN MODEMS OF DISCRETE FREQUENCY SIGNALS

Asp. Ivanov A.V.

Omsk Scientific Research Institute of Instrument Engineering
Omsk State Technical University

The paper considers a method for estimating the average energy level of additive white Gaussian noise (hereinafter referred to as ABGSH) for modems of discrete frequency (hereinafter referred to as RF) signals. The new method is based on the analysis of the energy distribution density in the RF matrix. A brief overview of noise energy estimation methods applicable to RF signal modems is provided. The main stages of the proposed method are described. The computational complexity of the algorithms allowing the implementation of the new method is considered. A comparison is made between the theoretical computational efficiency of the new method and the method based on ordinal statistics. A theory is put forward about the robustness of the new method and its self-sufficiency for use in RF signal modems, and cases where the use of the new method is limited are also considered.



ВЛИЯНИЕ НА НАДЕЖНОСТЬ ДЕКАМЕТРОВОГО КАНАЛА СВЯЗИ ПРИМЕНЕНИЯ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ В УСЛОВИЯХ ДИФFUЗНОСТИ ИОНОСФЕРЫ

проф. д.т.н. Пашинцев В.П.,¹

к.т.н. Белоконов Д.А.²

¹Северо-Кавказский федеральный университет

²Краснодарское высшее военное училище

В современных системах цифровой радиосвязи декаметрового диапазона широко применяются методы бинарной частотной модуляции и многократной фазовой и квадратурно-амплитудной модуляции. Известны методы оценки помехоустойчивости и надежности связи в однолучевом декаметровом канале связи с диффузной многолучевостью и райсовскими замираниями. Однако эти методы ограничены применением сигналов без использования помехоустойчивого кодирования. В докладе показано влияние применения помехоустойчивого кодирования блочных кодов Рида-Соломона и сверточных кодов на надежность декаметрового канала связи в условиях диффузности ионосферы.

Известно [1, 2], что надежность декаметровой (ДКМ) связи описывается как вероятность того, что с достоверность (или вероятность ошибки $P_{\text{ош}}$) приема сигналов будет не хуже допустимого значения ($P_{\text{ош,доп}}$):

$$D_{\text{св}} = P(P_{\text{ош}} \leq P_{\text{ош,доп}}) = F([\bar{Z} - Z_{\text{доп}}]/\sigma_Z) = F(\Delta Z/\sigma_Z) = F(\xi). \quad (1)$$

Здесь $F(\xi) = (\sqrt{2\pi})^{-1} \int_{-\infty}^{\xi} \exp(-0,5t^2) dt$ – функция Лапласа; $\xi = (\bar{Z} - Z_{\text{доп}})/\sigma_Z = \Delta Z/\sigma_Z$; $\bar{Z}$ – среднее (медианное) отношение (превышение) сигнал/шум (СШ) на входе приемника (ПРМ), в условиях замираний, равное отношению СШ при отсутствии замираний ($Z = \bar{Z}$), выраженное в децибелах (дБ); $Z_{\text{доп}}$ – допустимое превышение СШ на входе ПРМ, определяемое по функциональной зависимости $P_{\text{ош}} = \psi(Z = \bar{Z})$ при $P_{\text{ош}} = P_{\text{ош,доп}}$ в условиях интерференционных замираний принимаемых сигналов; σ_Z – среднеквадратическое отклонение (СКО) превышения СШ при медленных замираниях сигналов и помех. Входящее в выражение (1) СКО превышения С/П при медленных замираниях сигналов и помех от выбора рабочей частоты не зависит (т.е. $\sigma_Z(f_0) = \sigma_Z$) и в среднем за месяц составляет $\sigma_Z = 14$ дБ[3].

Известно [4-6], что для повышения надежности ДКМ связи применяется разнесенный прием на несколько антенн, который позволяет уменьшить допустимое отношение С/Ш. Но в то же время, эффективным способом уменьшения допустимого отношения С/Ш является применение помехоустойчивого кодирования [5-7]. В современных ДКМ системах связи применяются коды Рида-Соломона и сверточные коды [8-9]. Известны [10] методики оценки надежности ДКМ канала связи в условиях диффузности ионосферы ($\beta_{\text{и}}$) с цифровыми видами модуляции сигналов, такие как фазовая модуляция (PSK) и квадратурно-амплитудная модуляция (QAM) с кратностью M .

Однако методика, позволяющая оценить надежность ДКМ канала связи с цифровыми видами модуляции и применением помехоустойчивого кодирования в зависимости от степени диффузности ионосферы и выбора рабочей частоты отсутствует.

Целью доклада является оценка влияния на надежность ДКМ канала связи применения помехоустойчивого кодирования в условиях диффузности ионосферы.

Известно, что в ДКМ радиосвязи в 90 % преобладают замирания сигнала, распределенные по закону Райса [11, 12]. Известно выражение для оценки параметра Райса в зависимости от выбора отношения рабочей частоты к МПЧ и уровня диффузности ионосферы [13]:

$$\gamma^2 = (\exp(\pi(f_0/f_m)\beta_{\text{и}}f_m/cK_s^2 \sec^2 \varphi_0)^2 \sqrt{\pi} r_0 L_3) - 1)^{-1}, \quad (2)$$

где c – скорость света; K_s – поправочный коэффициент на сферичность Земли и ионосферы; φ_0 – угол падения волны на нижнюю границу отражающего слоя F ионосферы; r_0 – характерный (средний) размер мелкомасштабных ионосферных неоднородностей (200...500 м); L_3 – эквивалентный однородный путь волны в слое F2 ионосферы (зависящий от его критической частоты f_{F2} , $\beta_{\text{и}}$ степень диффузности ионосферы, высоты нижней границы и максимума ионизации слоя F2 ионосферы, дальности радиосвязи). Входящие в (2) параметры L_3 , K_s , φ_0 так же зависят от f_0 . Более детальное описание этих функциональных зависимостей приведено в [14].

Известен метод [5] позволяющий оценить помехоустойчивость цифровых сигналов с применением помехоустойчивого кодирования в канале связи с замираниями Райса, основу данного метода составляет выражение:

$$P_{\text{ош}} = \int_0^{\infty} P_{\text{ош}}^{\text{AWGN}}(h^2) \cdot P_{\xi}(h^2, \gamma^2, \Omega) dh^2, \quad (3)$$

где $P_{\text{ош}}^{\text{AWGN}}$ – вероятность ошибки на бит цифровых сигналов с кодированием в канале с аддитивным белым гауссовским шумом, P_{ξ} – плотность распределения Райса.

Выражение плотности распределения Райса [5, 6]:

$$P_{\xi} = \frac{2h^2(\gamma^2 + 1)}{\Omega} \exp\left(-\frac{(\gamma^2 + 1)h^4}{\Omega} - \gamma^2\right) I_0\left(2h^2 \sqrt{\frac{\gamma^2(\gamma^2 + 1)}{\Omega}}\right). \quad (4)$$

Данный метод основывается на численных методах решения, в частности он реализован в стандартных библиотеках численных методов MATLAB для оценки помехоустойчивости приема сигналов BERTOOL [15]. Известны [16, 17] работы по оценке помехоустойчивости цифровых сигналов с кодированием в канале с замираниями Релея, где применяется данный метод.

Известно [5, 7, 18, 19], выражение для оценки помехоустойчивости цифровых сигналов в канале с аддитивным белым гауссовским шумом (AWGN) и применением кодирования Рида-Соломона:

$$P_{\text{ош}} \approx \frac{2^{q-1}}{(2^q - 1)N} \sum_{m=t+1}^N m \binom{N}{m} (P_s)^m (1 - P_s)^{N-m}, \quad (5)$$

где $q = \log_2 M$ – число бит в одном закодированном символе, $N = 2^q - 1$ – длина кодового слова в символах, $t = (N - K)/2$ – максимально исправляемое число ошибочных символов, здесь K – длина информационной части в символах, P_s – вероятности ошибки на символ без кодирования, m – число ошибочных символов в одном кодовом слове, $\binom{N}{m}$ – число способов выбрать m ошибочных символов из N .

Известно [5, 7], выражение для оценки помехоустойчивости цифровых сигналов QAM-M в канале с аддитивным белым гауссовским шумом и применением сверточного кодирования:

$$P_{\text{ош}} \approx \sum_d^{\infty} B_d P_2(d), \quad (6)$$

где d выходное расстояние Хэмминга, B_d – суммарное среднее число ошибочных информационных битов по всем путям веса d , $P_2(d)$ – вероятность ошибочного выбора пути длины d . Для «жесткого» решения $P_2(d)$:

$$P_2(d) = \sum_{k=\frac{d+1}{2}}^d \binom{d}{k} p^k (1-p)^{d-k}, \quad (7)$$

где k число ошибок на пути d , $\binom{d}{k}$ – число способов выбрать ровно k ошибочных позиций из d , p – вероятности ошибки на символ без кодирования после демодуляции.

На основе графика, представленного на рисунке 1, и выражений (3-6) на рисунке 2 показаны зависимости помехоустойчивости цифровых сигналов QAM с кратностью $M=64$ с кодированием Рида-Соломона (линия 1) и сверточным кодированием (линия 2) в канале с замираниями Райса при $\gamma^2=0, 5$. Параметры кодирования выбраны произвольно, для кодирования Рида-Соломона выбрано $N=255$ и $K=223$ (255, 223), для сверточного кода $d=10$ и $k=7$. На этом же рисунке показаны известные [20] графики помехоустойчивости цифровых сигналов QAM-M без кодирования в канале связи с замираниями Райса (пунктирная линия 3).

Рисунок 1.

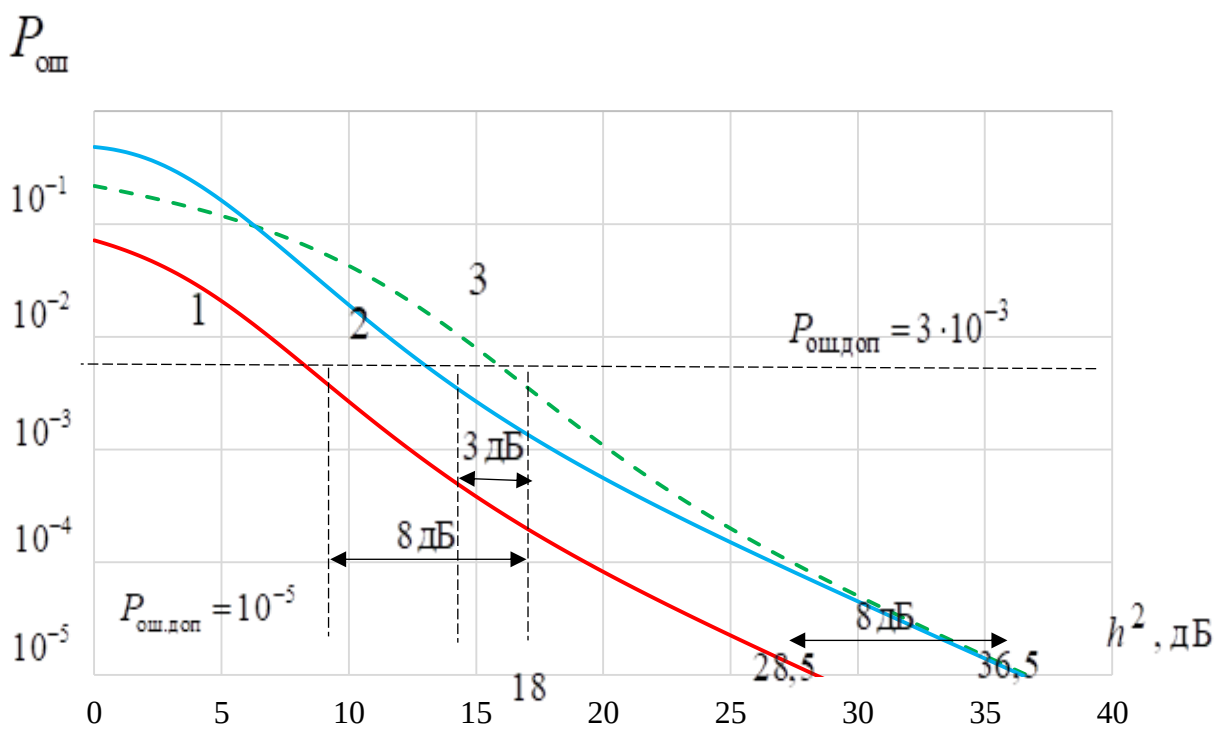
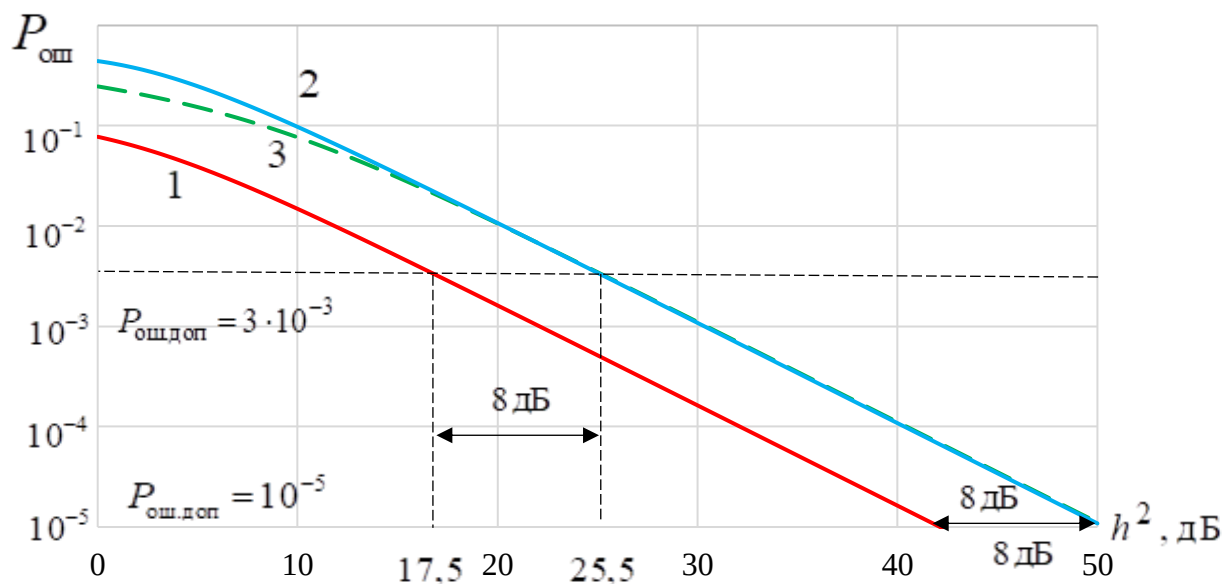


Рисунок 2. Зависимость $P_{\text{ош}}(h^2, \gamma^2)$ помехоустойчивости сигналов QAM с кратностью $M=64$ с кодами Рида-Соломона (линия 1), с использованием сверточных кодов (линия 2) и без кодирования (пунктирная линия 3) при а) $\gamma^2 = 0$, б) $\gamma^2 = 5$

На основе известных графиков [13] $\gamma^2(f_0/f_M, \beta_{\text{и}})$ для случая нормальной диффузности $\beta_{\text{и}} = 5 \cdot 10^{-3}$ и выражений (3-6) графическим методом определяется зависимость допустимого отношения $C/\Pi Z_{\text{доп}}(f_0/f_M, \beta_{\text{и}})$ от выбора отношения рабочей частоты к МПЧ и уровня диффузности ионосферы при современных требованиях к допустимой вероятности ошибки $P_{\text{ош,доп}} = 10^{-5}$ представлена на рисунке 3.

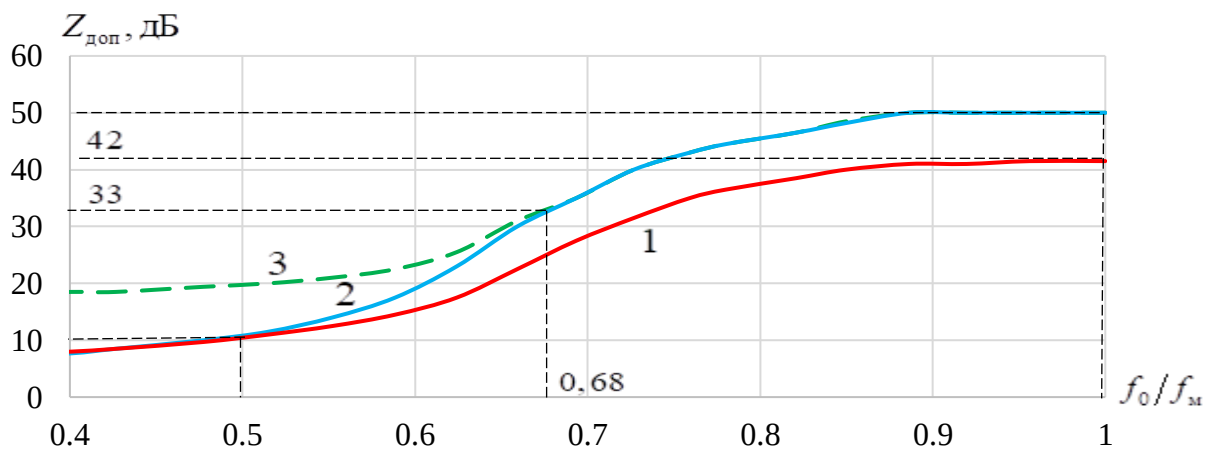


Рисунок 3. Зависимости $Z_{\text{доп}}$ допустимого отношения сигналов QAM с кратностью $M=64$ с кодами Рида-Соломона (линия 1), с использованием сверточных кодов (линия 2) и без кодирования (пунктирная линия 3) от отношения рабочей частоты к МПЧ при нормальной диффузности $\beta_{\text{и}} = 5 \cdot 10^{-3}$

Анализ графиков, представленных на рисунке 3, показывает, что в условиях нормальной диффузности ионосферы ($\beta_{\text{и}} = 5 \cdot 10^{-3}$) допустимое отношение С/Ш при отношении рабочей частоты к МПЧ $f_0/f_M=1$ для сигналов QAM-64 с кодами Рида-Соломона составляет $Z_{\text{доп}}=42$ дБ, для случая использования сверточных кодов допустимое отношение составит $Z_{\text{доп}}=50$ дБ, для случая без использования кодирования допустимое отношение С/Ш, также составит $Z_{\text{доп}}=50$ дБ. Допустимое отношение С/Ш для случая использования сверточных кодов и без кодирования будут совпадать в диапазоне отношения рабочей частоты к МПЧ $\Delta f_0/f_M=0,68 \dots 1$, при отношении рабочей частоты к МПЧ $f_0/f_M=0,68$ допустимое отношение С/Ш составит $Z_{\text{доп}}=33$ дБ. А при диапазоне отношения рабочей частоты к МПЧ от $f_0/f_M=0,5$ и ниже, значения допустимого отношения С/Ш будут совпадать для случая использования сверточных кодов и кодов Рида-Соломона, при отношении рабочей частоты к МПЧ $f_0/f_M=0,5$ допустимое отношение С/Ш составит $Z_{\text{доп}}=10$ дБ.

На основе рисунков 3 и выражения (1) на рисунке 4 показаны графики надежности ДКМ канала связи цифровых сигналов QAM-64 $D_{\text{св}}(f_0/f_M, \beta_{\text{и}})$ с применением помехоустойчивого кодирования Рида-Соломона (линия 1), сверточных кодов (линия 2) и без кодирования (пунктирная линия 3). Значение $\bar{Z}$ для расчетов взято из известных [3] графиков зависимости $\bar{Z}(f_0/f_M)$ от отношения рабочей частоты к МПЧ.

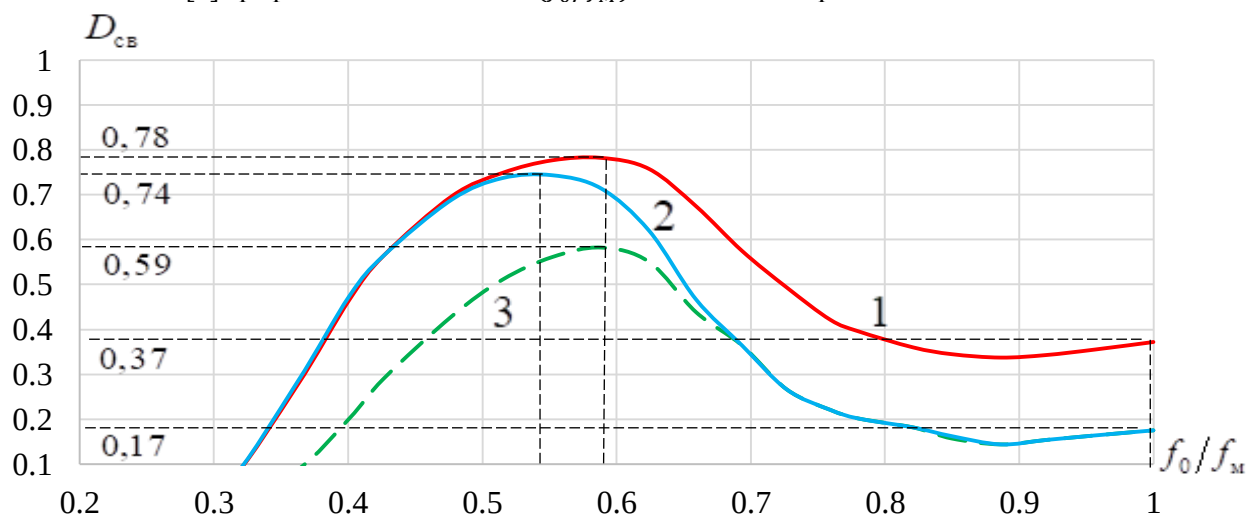


Рисунок 4. Зависимость $D_{\text{св}}(f_0/f_M, \beta_{\text{и}})$ надежности ДКМ канала связи от отношения рабочей частоты к МПЧ при нормальной диффузности ионосферы для сигналов QAM с кратностью $M=64$ с кодами Рида-Соломона (линия 1), с использованием сверточных кодов (линия 2) и без кодирования (пунктир. линия 3).

Анализ графиков представленных на рисунке 4, показывает, что в условиях нормальной диффузности ионосферы ($\beta_{\text{и}} = 5 \cdot 10^{-3}$) надежность ДКМ канала связи при отношении рабочей частоты к МПЧ $f_0/f_M=1$ для сигналов QAM-64 с кодами Рида-Соломона составляет $D_{\text{св}}=0,37$, для случая использования сверточных кодов надежность ДКМ канала связи составит $D_{\text{св}}=0,17$, для случая без использования кодирования надежность ДКМ канала связи, также составит $D_{\text{св}}=0,17$. Максимальное значение надежности ДКМ канала

связи для сигналов QAM-64 с кодами Рида-Соломона составляет $D_{св}=0,78$ и достигается при отношении рабочей частоты к МПЧ $f_0/f_M=0,59$, для случая использования сверточных кодов максимальная надежность ДКМ канала связи составит $D_{св}=0,74$ при отношении рабочей частоты к МПЧ $f_0/f_M=0,53$, для случая без использования кодирования максимальная надежность ДКМ канала связи составит $D_{св}=0,59$ при отношении рабочей частоты к МПЧ $f_0/f_M=0,59$. Таким образом, разница между максимальным значением надежности ДКМ канала связи с сигналами QAM-64 для случая использования кодов Рида-Соломона и без кодирования составляет: $\Delta D_{св}=0,78-0,59=0,15$ или 19,2 %. Разница надежности ДКМ канала связи для случая кодов Рида-Соломона и без кодирования составит: $\Delta D_{св}=0,78-0,59=0,15$ или 19,2 %. При отношении рабочей частоты к МПЧ от $f_0/f_M=0,5$ и ниже значения надежности ДКМ канала связи для случая использования кодов Рида-Соломона и сверточных кодов будут совпадать, а при отношении рабочей частоты к МПЧ от $f_0/f_M=0,5$ и до МПЧ значения надежности ДКМ канала связи для случая использования сверточных кодов будут и случая без кодирования будут совпадать.

Закключение

Таким образом, проведена оценка влияния применения помехоустойчивого кодирования на надежность ДКМ канала связи в условиях диффузности ионосферы. Установлено, что в условиях нормальной диффузности наибольшую надежность ДКМ канала связи ($D_{max}=0,78$) дает применение кодов Рида-Соломона, которая достигается при отношении рабочей частоты к МПЧ $f_0/f_M=0,59$. При отношении рабочей частоты к МПЧ $f_0/f_M=1$ значение надежности ДКМ канала связи с применением кодов Рида-Соломона составляет $D_{св}=0,37$, что на 0,2 больше, чем для случая применения сверточных кодов и случая без кодирования. Применение кодов Рида-Соломона позволяет значительно повысить (на 19,2 %) надежность ДКМ канала связи относительно случая без кодирования и на 5,1 % относительно сверточных кодов. Это обусловлено тем, что разница допустимого отношения С/Ш $Z_{доп}$ между случаем применения кодов Рида-Соломона будет ниже на 8 дБ относительно случая ДКМ канала связи с цифровыми сигналами QAM-64. Отсюда можно сделать вывод, что применение кодов Рида-Соломона и сверточных кодов позволяет повысить надежность ДКМ канала связи с цифровыми сигналами в условиях диффузности ионосферы, однако пропускная способность ДКМ канала связи будет ниже[5] из-за добавления избыточности при кодировании сигнал.

Литература

1. Комарович, В. Ф. Случайные помехи и надежность КВ связи / В. Ф. Комарович, В. Н. Сосунов. – Москва : Связь, 1977. – 136 с. – Текст : непосредственный.
2. Мешалкин, В. А. Поля и волны в задачах разведзащищенности и радиоэлектронной защиты систем связи / В. А. Мешалкин, Б. В. Сосунов, В. В. Филиппов. – Санкт-Петербург : ВАС, 1993. – 332 с. – Текст : непосредственный
3. Пашинцев, В. П. Зависимость надежности связи в дециметровом радиоканале от выбора рабочей частоты с учетом сигнально-помеховой обстановки и диффузности ионосферы / В. П. Пашинцев, А. Д. Скорик, С. А. Коваль, Д. П. Киселев. – Текст : непосредственный // Системы управления, связи и безопасности. – 2019. – № 4. – С. 300–322.
4. Андронов, И. С. Передача дискретных сообщений по параллельным каналам / И. С. Андронов, Л. М. Финк. – Москва : Советское радио, 1971. – 408 с. – Текст : непосредственный.
5. Proakis, J. G. Digital Communications / J. G. Proakis. – New York : McGraw-Hill, 2001. – 1002 p. – Text : direct.
6. Mathuranathan, V. Wireless Communication Systems in Matlab / V. Mathuranathan // Second Edition. – Independently published, 2020. – P. 382.
7. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение: перевод с английского / Б. Скляр. – Москва: Вильямс, 2003. – 1104 с. – Текст: непосредственный.
8. Рыбаков А. И. Помехоустойчивая сигнально-кодовая конструкция на базе частотной манипуляции в ионосферном канале радиосвязи [Электронный ресурс] // Экономика и качество систем связи. – 2023. – № 1. – С. 29–33.
9. Егоров В. В. Высокоскоростные адаптивные КВ системы передачи данных [Электронный ресурс] // Электросвязь. – 2015. – № 6. – С. 59–62.
10. Белоконов, Д. А. Устройство прогнозирования надежности связи при приеме цифровых сигналов в дециметровом канале связи в условиях диффузности ионосферы / Д. А. Белоконов, В. П. Пашинцев, И.А. Скрипак, С.А. Коваль – Текст : непосредственный // Радиоэлектронные устройства и системы для инфокоммуникационных технологий – REDS-2025 : доклады 80-й Международной конференции. – Москва : РНТОРЭС им. А. С. Попова, 2024. – С. 209–213.

11. Кириллов, Н. Е. Помехоустойчивая передача сообщений по линейным каналам со случайно изменяющимися параметрами / Н. Е. Кириллов. – Москва: Советское радио, 1971. – 256 с.
12. Кловский, Д. Д. Теория передачи сигналов / Д. Д. Кловский. – Москва: Связь, 1973. – 376 с.
13. Методика оценки влияния диффузности ионосферы и выбора рабочей частоты на помехоустойчивость коротковолновой связи / В. П. Пашинцев, Д. А. Белоконов, В. А. Цимбал и др. – Текст : электронный // Журнал радиоэлектроники. – 2024 – № 12. – URL: <http://jre.cplire.ru/jre/dec24/2/text.pdf>. (дата обращения: 28.03.2026).
14. Расчет параметра глубины замираний в однолучевой декаметровой радиолнии / В. П. Пашинцев, С. А. Тишкин, А. И. Иванников, И. И. Боровлев. – Текст : непосредственный // Известия вузов России. Радиоэлектроника. – 2001. – Т. 44, № 12. – С. 57–65.
15. Описание функции MATLAB / Analytical Expressions Used in berfading Function and Bit Error Rate Analysis App. – URL: <https://www.mathworks.com/help/comm/ug/analytical-expressions-used-in-berfading-function-and-bit-error-rate-analysis-app.html> (дата обращения: 14.04.2025). – Текст : электронный.
16. Implementation and Bit Error Rate analysis of BPSK Modulation and Demodulation Technique using MATLAB [Электронный ресурс] // International Journal of Engineering Trends and Technology (IJETT). – 2013. – Vol. 4, No. 9.
17. Webb W. T., Hanzo L., Steele R. Bandwidth efficient QAM schemes for Rayleigh fading channels // IEE Proceedings I – Communications, Speech and Vision. – 1991. – Vol. 138, No. 3. – P. 169–175.
18. Gulliver T. A. Matching Q-ary Reed-Solomon codes with M-ary modulation // IEEE Transactions on Communications. – 1997. – Vol. 45, No. 11. – P. 1349–1353.
19. Simon, M. K. Digital Communication over Fading Channels: A Unified Approach to Performance Analysis / M. K. Simon, M. S. Alouini. – New York : John Wiley & Sons, 2000. – 544 p.
20. Пашинцев, В. П. Методика оценки помехоустойчивости приема цифровых сигналов в коротковолновом канале связи с учетом диффузности ионосферы / В. П. Пашинцев, Д. А. Белоконов. – Текст: непосредственный // Информационные технологии. – 2025. – Т. 31.

INFLUENCE OF THE USE OF ERROR-CORRECTING CODING ON THE RELIABILITY OF A DECAMETER COMMUNICATION CHANNEL UNDER DIFFUSE IONOSPHERIC CONDITIONS

North Caucasus Federal University

DR., Prof. Pashintsev V.P.,

Krasnodar Higher Military School

PhD, Belokon D.A

In modern digital decameter-band radio communication systems, methods of binary frequency modulation and various forms of multilevel phase and quadrature-amplitude modulation are widely used. Known methods exist for estimating interference immunity and communication reliability in a single-path decameter communication channel with diffuse multipath propagation and Ricean fading. However, these methods are limited to the use of signals without applying error-correcting coding. The report demonstrates the effect of using error-correcting coding with Reed–Solomon block codes and convolutional codes on the reliability of a decameter communication channel under ionospheric diffusion conditions.



ГИБРИДНЫЕ РАДИО-ОПТИЧЕСКИЕ СИСТЕМЫ СВЯЗИ ДЛЯ ГРУППИРОВОК БЛА

асп. Кадочников Д.М.¹, проф., доц., д.т.н. Страхов С.Ю.¹,
доц., к.т.н. Сотникова Н.В.¹, к.т.н. Брусенцов К.А.²

¹Балтийский государственный технический университет «Военмех» им. Д. Ф. Устинова
²ООО «Пантес МТ»

В работе рассматривается задача организации устойчивого информационного обмена в самоорганизующихся сетях беспилотных летательных аппаратов (БПЛА) в условиях нестабильной среды распространения сигнала. Объектом исследования является гибридная система связи, объединяющая атмосферный оптический (1550 нм) и радиочастотный (2.4 ГГц) каналы передачи данных. Разработана имитационная модель, учитывающая затухание оптического излучения в дисперсных средах (туман, дождь), влияние атмосферной турбулентности и ошибки наведения, вызванные случайными колебаниями носителя. Представлены результаты численного моделирования вероятности битовой ошибки (BER) и вероятности срыва связи в зависимости от дистанции между узлами и метеорологических условий. Анализ полученных данных показывает, что использование гибридной схемы с переключением на резервный радиоканал позволяет поддерживать соединение с заданным уровнем надежности на дистанциях до 1,2 км в условиях, критических для функционирования каналов связи.

В последние десятилетия наблюдается активное внедрение беспилотных летательных аппаратов (БПЛА) для решения задач мониторинга, ретрансляции сигналов и поисково-спасательных операций. Объединение одиночных аппаратов в самоорганизующиеся сети (FANET — Flying Ad-hoc Networks) позволяет повысить эффективность выполнения задач за счет распределения полезной нагрузки и сенсорных возможностей. Однако критическим условием функционирования таких группировок является обеспечение надежного высокоскоростного канала связи между узлами [1].

Традиционно для организации связи в группах БПЛА используются радиочастотные (РЧ) каналы. Несмотря на низкую стоимость и простоту реализации, РЧ-технологии обладают рядом существенных ограничений: дефицит частотного спектра, низкая защищенность от преднамеренных помех и перехвата, а также ограниченная скорость передачи данных, которая становится «узким местом» при передаче потокового видео высокого разрешения или программно-определяемых радиосистем [2]. К этому списку проблем добавляется специфика распространения радиоволн на малых высотах (10–70 м), характерных для работы группировок малых БПЛА. В этих условиях значительное влияние эффект многолучевого распространения: сигнал, отраженный от подстилающей поверхности (земли), складывается с прямым сигналом в противофазе, что приводит к появлению зон глубоких замираний (федингу) и резкому падению на входе приемника. Результаты моделирования влияния этого эффекта на уровень сигнала для высот 10–70 м и на частоте 5,8 ГГц представлены на рисунке 1.

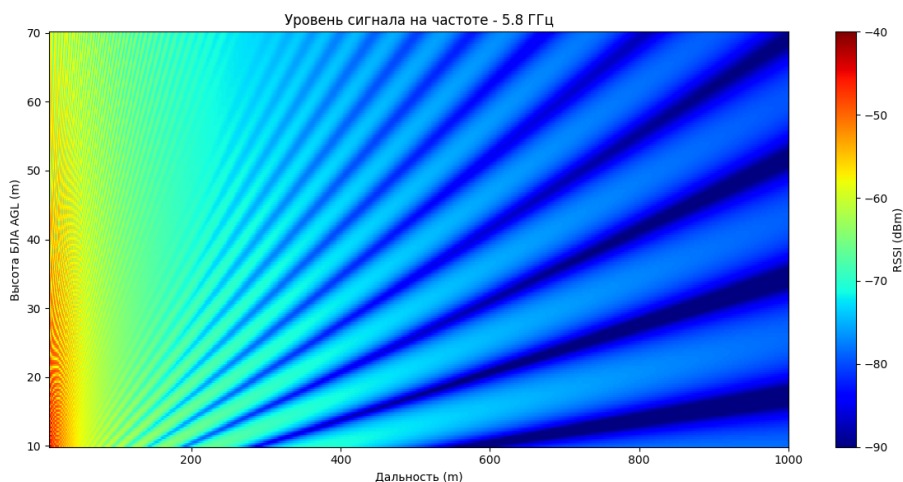


Рисунок 1 — Результат моделирования РЧ канала между БЛА на малых высотах

Альтернативой радиоканалу выступают атмосферные оптические линии связи (АОЛС). Использование оптического диапазона обеспечивает значительно более высокую пропускную способность (до нескольких Гбит/с), высокую скрытность передачи благодаря узкой диаграмме направленности. Тем не менее, работа

АОЛС критически зависит от состояния атмосферного канала. Такие факторы, как гидрометеоры (туман, дождь, снег) и атмосферная турбулентность, вызывают затухание и флуктуации интенсивности оптического сигнала (сцинтилляции). Кроме того, при применении их на подвижных объектах (БПЛА) возникают ошибки наведения, вызванные колебаниями платформы и маневрами аппарата, что может привести к невозможности установления оптического соединения [3].

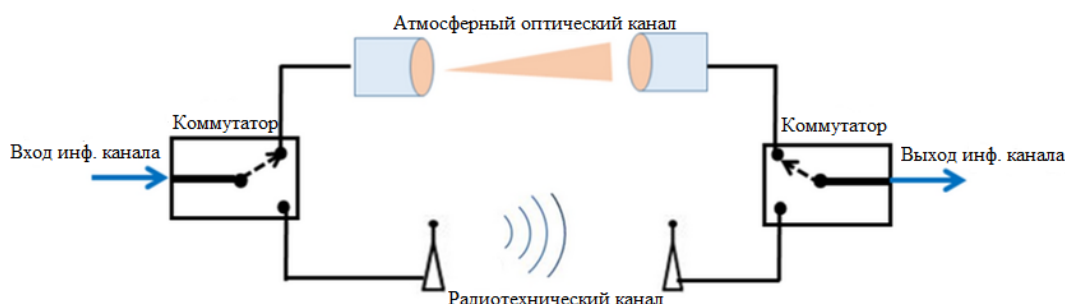


Рисунок 2 — Схема гибридной системы связи

Перспективным решением для нивелирования недостатков отдельных технологий является внедрение гибридных систем, схема которой представлена на рисунке 2, где АОЛС служит основным высокоскоростным каналом, а РЧ — резервным, активируемым при деградации оптического сигнала. Это объединяет высокую пропускную способность оптики с всепогодной надежностью радиосвязи. Существующие исследования гибридных систем часто рассматривают стационарные сценарии (связь между зданиями) и не учитывают в полной мере совокупное влияние атмосферной турбулентности и динамических ошибок наведения, характерных для малоразмерных БПЛА.

Целью данной работы является моделирование гибридного канала связи в условиях динамического изменения дистанции и параметров среды, а также анализ эффективности переключения каналов для поддержания заданного уровня вероятности ошибки (BER).

Оптическое излучение в разрабатываемой модели описывается в виде гауссова пучка, подверженного уширению в турбулентной среде. Расчет коэффициента затухания сигнала базируется на эмпирической модели Кима, позволяющей связать потери оптической мощности с метеорологической дальностью видимости на трассе:

$$\gamma = \frac{17}{V} \left(\frac{\lambda}{550} \right)^{-q},$$

где V — метеорологическая дальность видимости (км), λ — длина волны (нм), q — коэффициент рассеяния, зависящий от V .

Особое внимание в исследовании уделено оценке геометрических потерь, индуцированных механической нестабильностью полетной платформы. Смещение энергетического центра лазерного луча относительно фокальной плоскости приемной апертуры рассматривается как двумерная стохастическая величина, подчиняющаяся распределению Рэлея. При этом среднеквадратичное отклонение системы пространственной стабилизации (джиттер) задано на уровне:

$$h_g \approx \left(\frac{D}{\omega_z} \right)^2 e^{\left(-\frac{2r^2}{\omega_z^2} \right)},$$

где D — диаметр апертуры (м), ω_z — радиус пучка на расстоянии z (м), а смещение r описывается распределением Рэлея с дисперсией σ_j^2 .

В качестве передающего устройства в модели использован лазерный диод с длиной волны 1550 нм и средней мощностью 30 дБм (1 Вт). Выбор данного диапазона продиктован требованиями международных стандартов лазерной безопасности (IEC 60825-1) и широкой доступностью оборудования для волоконно-оптических систем связи.

Для компенсации вибрационных нагрузок и ошибок трекинга в параметры передатчика заложена начальная угловая расходимость пучка 40 мрад. Такой подход представляет собой классический компромисс: уширение диаграммы направленности приводит к квадратичному падению плотности мощности, однако гарантирует попадание пятна засветки в приемную апертуру диаметром $D=0,05$ м даже при резких пространственных флуктуациях носителя (рисунок 3). Подобное расширение диаметра пучка

позволяет ограничить среднее вносимое затухание на уровне 3 дБ при характерных для малых БПЛА амплитудах раскачки.

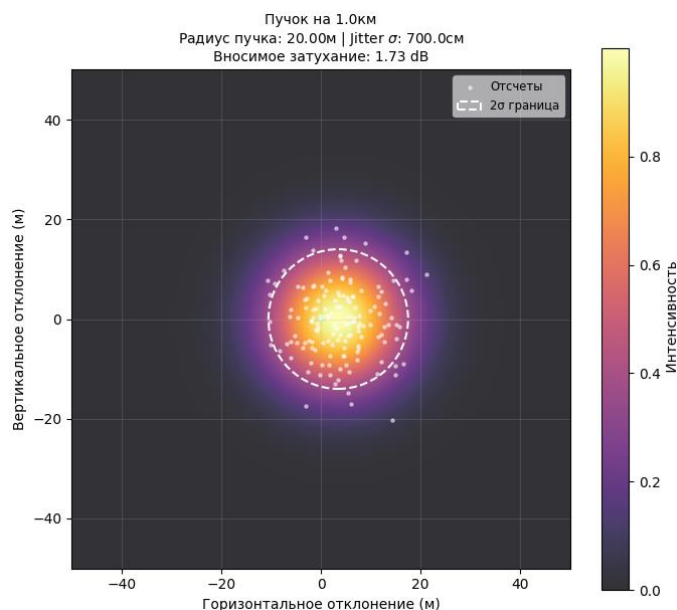


Рисунок 3 — Визуализация пучка на дистанции 1 км

Приемный оптический тракт построен на базе высокочувствительного лавинного фотодиода (ЛФД) с токовой чувствительностью 0,8 А/Вт и полосой пропускания 1 ГГц, что обеспечивает информационную скорость до 0,5 Гбит/с. Комплексная оценка отношения сигнал/шум (SNR) производится с учетом аддитивного белого гауссова шума (AWGN), включающего тепловой и дробовой компоненты, эквивалентную мощность внутреннего шума приемника ($NEP = 10^{-12}$ Вт)

$$SNR = \frac{(R * P_r)^2}{(NEP * R)^2 * B},$$

где R — токовая чувствительность ЛФД (А/Вт), P_r — принятая оптическая мощность (Вт), NEP — эквивалентную мощность внутреннего шума приемника (Вт), B — полоса пропускания (Гц).

На основе вычисленного значения SNR определяется итоговая вероятность битовой ошибки (BER) для амплитудной модуляции OOK (On-Off Keying), применяемой в оптическом модеме:

$$BER = \frac{1}{2} * erfc\left(\frac{\sqrt{SNR}}{2\sqrt{2}}\right),$$

где SNR — отношение сигнал/шум.

Численное моделирование проведено для диапазона дистанций от 100 м до 1,2 км с охватом различных атмосферных сценариев: от идеальных условий «ясного неба» (видимость 50 км) до густого тумана (видимость 0,5 км) и режимов сильной оптической турбулентности ($C_n^2=10^{-3}$)

Пороговым значением работоспособности высокоскоростного оптического линка (155 Мбит/с) принят уровень $BER \leq 10^{-4}$ (до применения алгоритмов прямой коррекции ошибок FEC).

Анализ результатов показывает, что в условиях оптической прозрачности энергетики АОЛС с запасом хватает для обеспечения $BER \sim 10^{-8}$ на максимальной дальности 2 км. Искусственно уширенная диаграмма направленности успешно нивелировала до 97% флуктуаций луча, вызванных ветровым сносом. Однако при появлении густого тумана удельное затухание сигнала экспоненциально возрастает (свыше 45 дБ/км), что ведет к необратимой деградации канала ($BER > 10^{-3}$) уже на дистанциях 650–700 м. Аналогичным образом, интенсивные осадки (дождь 25 мм/ч) сокращают радиус уверенного оптического контакта до 1,1 км за счет эффектов Ми-рассеяния (рисунок 4).

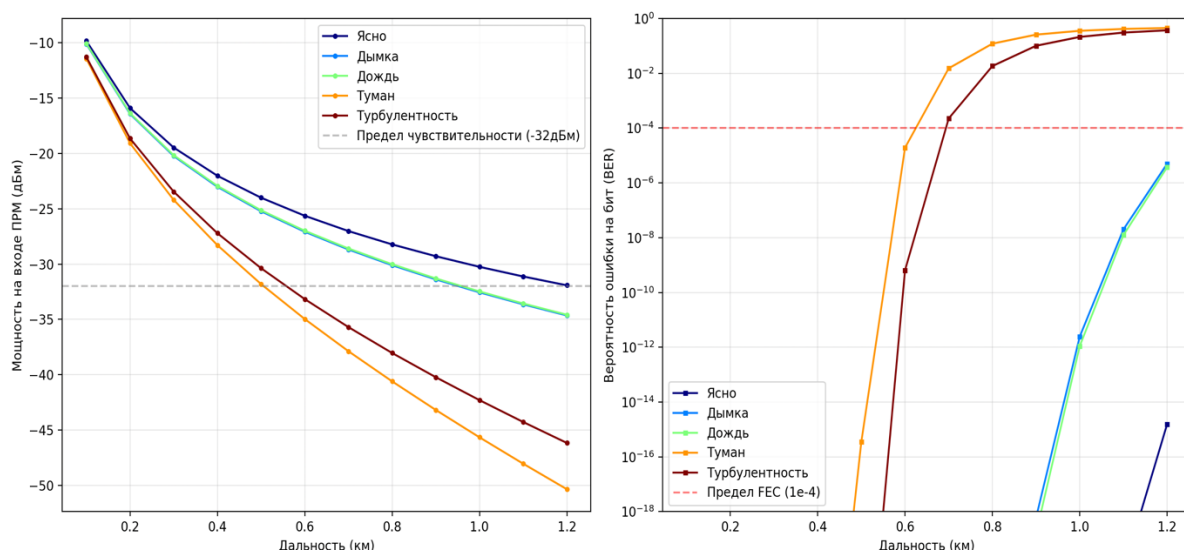


Рисунок 4 — Результат моделирования АОЛС

Для обеспечения отказоустойчивости сети FANET в модель интегрирована логика автоматического переключения (Hard Handover) на резервный РЧ-канал (2,4 ГГц). Результат работы гибридного канала представлен на рисунке 5. Алгоритм инициирует смену физической среды передачи при снижении SNR в одном канале ниже другого. Для исключения эффекта «пинг-понга» (частых хаотичных переключений туда-обратно при флуктуациях сигнала около порога) в систему управления введен временной гистерезис.

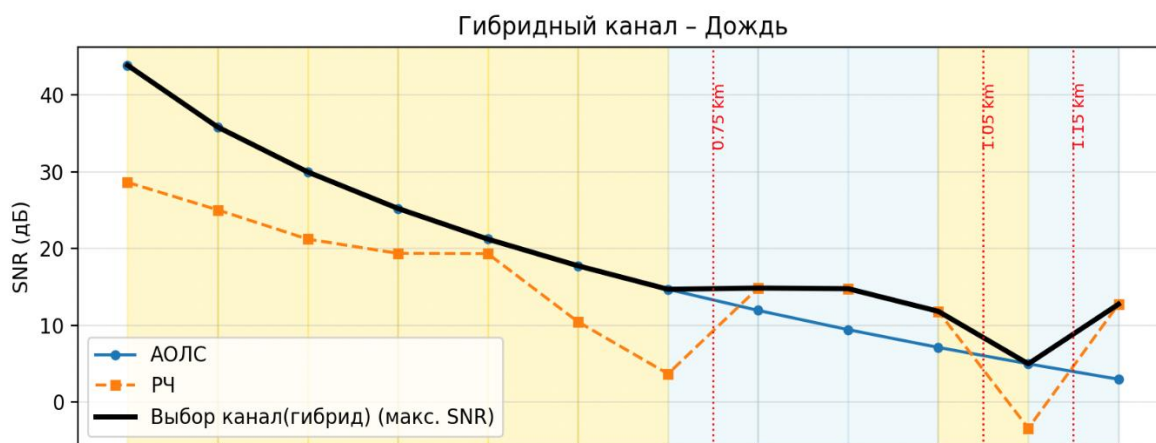


Рисунок 5 — Результат работы гибридного канала на малых высотах

Разработанная модель подтвердила, что уширение лазерного пучка до 40 мрад позволяет успешно компенсировать пространственные флуктуации носителя и поддерживать высокоскоростную передачу данных на дистанциях до 1 км в условиях прозрачной атмосферы. При ухудшении метеорологической обстановки (туман, дождь) дальность уверенного приема оптического сигнала неизбежно сокращается до 400-550 м, что компенсируется алгоритмом автоматического перевода трафика на резервный радиочастотный канал (2,4 ГГц). Стабильное функционирование резервной линии на малых высотах (10–70 м) достигается за счет применения OFDM-модуляции, компенсирующей интерференционные замирания, и адаптивного управления качеством обслуживания (QoS). Динамическая приоритизация важной телеметрической информации над ресурсоемкими потоками (видео) предотвращает перегрузку сети в моменты переключения каналов. В совокупности синергетическое объединение двух физических принципов передачи данных нивелирует уязвимости изолированных технологий связи и позволяет обеспечить надежное, непрерывное управление группировкой аппаратов при воздействии внешних факторов.

Литература

1. Матвеев С.А., Страхов С.Ю., Хромихин Д.А., Ким А.А., Дукельский К.В. Организация энергоинформационного обмена между устройствами управления формой трансформируемой

- антенны с применением волоконно-оптических технологий // Оптический журнал. 2016. Т. 83. № 11. С. 73–78.
2. Кочин Л.Б., Страхов С.Ю. Лазерная система передачи энергии и информации // В книге: Лазерно информационные технологии в медицине, биологии, геоэкологии и транспорте–2016. Труды XXIV Международной конференции. 2016. С. 15–16.
 3. Зуев В.Е. Распространение видимых и инфракрасных волн в атмосфере. М.: Советское радио, 1970. 496 с.
 4. Страхов С.Ю., Савин А.В., Сотникова Н.В., Орлов А.Е. Оценка влияния оптических неоднородностей атмосферы на точность позиционирования лазерного луча при вертикальном зондировании // Оптический журнал. 2025. Т. 92. № 2. С. 56–66.
<http://doi.org/10.17586/1023-5086-2025-92-02-56-66>
 5. Дж. Дауги Анализ химических лазерных систем, Аэрокосмическая техника, №2, 1990, сс. 53-59 6. Mandar Khanal, Mahamudul Hasan, Nikolaus Sterbentz, Ryen Johnson, Jesse Weatherly. Accuracy comparison of aerial lidar, mobile-terrestrial lidar, and UAV photogrammetric capture data elevations over different terrain types // Infrastructures. 2020. V. 5. P. 65. <https://doi.org/10.3390/infrastructures5080065>

HYBRID RADIO-OPTICAL COMMUNICATION SYSTEMS FOR UAV FORMATIONS

Postgraduate student Kadochnikov D.M.¹,
Prof., Assoc., Doctor of Technical Sciences Strakhov S.Yu.¹,
Assoc., Candidate of Technical Sciences Sotnikova N.V.¹,
Candidate of Technical Sciences Brusentsov K. A.²

¹Baltic State Technical University "Voenmeh" named after D. F. Ustinov

²Pantes MT LLC

The article considers the problem of organizing sustainable information exchange in self-organizing networks of unmanned aerial vehicles (UAVs) in conditions of unstable signal propagation. The object of study is a hybrid communication system combining atmospheric optical (1550 nm) and radio frequency (2.4 GHz) data transmission channels. A simulation model has been developed that takes into account the attenuation of optical radiation in dispersed mediums (fog, rain), the influence of atmospheric turbulence, and pointing errors caused by random vehicle movement. The results of numerical simulation of the bit error rate (BER) and the probability of communication failure depending on the distance between nodes and meteorological conditions are presented. Analysis of the data obtained shows that the use of a hybrid scheme with switching to a backup radio channel allows maintaining a connection with a specified level of reliability at distances of up to 1,2 km in conditions critical for the functioning of isolated communication channels.



УТОЧНЕННОЕ УСЛОВИЕ ОТСУТСТВИЯ ЧАСТОТНО-СЕЛЕКТИВНЫХ ЗАМИРАНИЙ И МЕЖСИМВОЛЬНОЙ ИНТЕРФЕРЕНЦИИ В КАНАЛЕ СПУТНИКОВОЙ СВЯЗИ ПРИ ВОЗМУЩЕНИЯХ ИОНОСФЕРЫ

асп. Диптан П.А.

Северо-Кавказский федеральный университет

Получены уточненные условия отсутствия частотно-селективных замираний и межсимвольной интерференции в канале спутниковой связи с заданной шириной спектра F при сужении полосы когерентности F_k замираний в условиях искусственных возмущениях ионосферы и реализации различного отношения сигнал-шум на входе приемника (7дБ, 15дБ и 23 дБ) по критерию снижения пропускной способности. Показано, что при реализации отношения сигнал/шум на входе приемника 7-15 дБ пропускная способность канала спутниковой связи уменьшается на 10% (относительно случая рэлеевских замираний) при выполнении $F \leq 0,55F_k$.

Известно [1, 2], что при ионосферных возмущениях в канале спутниковой связи при передаче узкополосных сигналов с высокой скоростью ($R = 1/T_s > 100$ кБод) возникают частотно-селективные замирания (ЧСЗ) сигналов, когда полоса частот (ширина спектра) сигнала F становится шире полосы когерентности канала связи F_k (т.е. $F > F_k$). По мере возрастания мелкомасштабных флуктуаций полного электронного содержания (ПЭС) при возмущениях ионосферы происходит возрастание глубины замираний, сужение полосы когерентности трансionoсферного канала связи F_k возрастает степень ЧСЗ принимаемого простого сигнала (т.е. отношение F/F_k) и степень межсимвольной интерференции (МСИ) ($1/T_s F_k$). Согласно [1, 2] при передаче по трансionoсферному каналу спутниковой связи с ограниченной полосой частот $F_k \leq 100$ кГц простых сигналов ($B_s = T_s F = 1$) с высокой скоростью ($R = 1/T_s > 100$ кБод) условия возникновения ЧСЗ и МСИ выполняются одновременно: $F/F_k = 1/T_s F_k > 1$. Исследования [1-3] показывают, что условие отсутствия ЧСЗ и МСИ в канале спутниковой связи записывается в виде: $F/F_k \leq 1$, или $F \leq F_k$.

Однако, в работе [4] при использовании в качестве критерия допустимого снижения относительной пропускной способности канала спутниковой связи из-за ЧСЗ и МСИ на 1%, сформулировано уточненное условие отсутствия ЧСЗ и МСИ в канале спутниковой связи в виде: $F/F_k \leq 0,15$, или $F \leq 0,15F_k$.

Целесообразно оценить максимальное отношение ширины полосы канала связи F к полосе когерентности замираний в канале F_k (F/F_k) при возмущениях ионосферы с точки зрения увеличения скорости передачи символов в канале, при использовании в качестве критерия допустимого снижения относительной пропускной способности канала спутниковой связи из-за возникновения частотно-селективных замираний и межсимвольной интерференции на 5-10%.

Представленная работа является развитием исследований автора [4-8].

Оценка пропускной способности канала спутниковой связи при возмущениях ионосферы, возникновении частотно-селективных замираний и межсимвольной интерференции

Проводимое исследование является продолжением работы [4]. Напомним, что для случая наклонного распространения радиоволн величина СКО флуктуаций фазового фронта выходной волны σ_φ зависит от СКО мелкомасштабных флуктуаций ПЭС ионосферы, угла наклона распространения радиоволны (здесь и далее будем рассматривать наклонное СКО ПЭС $\sigma_{\Delta N_T}(\theta) = \sigma_{\Delta N_T} \sec \theta$) и несущей частоты f_0 сигнала как [1, 2]

$$\sigma_\varphi = \left(\overline{\Delta \varphi^2}(\rho) \right)^{1/2} = 80,8 \pi \sigma_{\Delta N_T}(\theta) / c f_0 = 80,8 \pi \sigma_{\Delta N_T} \sec \theta / c f_0, [\text{рад}], \quad (1)$$

где $\Delta \varphi(\rho)$ – флуктуации (искажения) фазового фронта выходной волны, обусловленные мелкомасштабными флуктуациями интегральной электронной концентрации $\Delta N_T(\rho) = \int \Delta N(\rho, h) dh$ ионосферы, c – скорость света [м/с]. Входящая в (1) величина СКО мелкомасштабных флуктуаций ПЭС ионосферы определяется как [1, 2]

$$\sigma_{\Delta N_T} = \left(\overline{\Delta N_T^2}(\rho) \right)^{1/2} = \left(\pi^{1/2} l_s h_s \sigma_{\Delta N}^2 \right)^{1/2} = \left(\pi^{1/2} l_s h_s \right)^{1/2} \sigma_{\Delta N}, [\text{м}^2], \quad (1a)$$

где l_s – характерный (средний) размер мелкомасштабных неоднородностей ионосферы [м], h_s – эквивалентная толщина ионосферы [м], $\sigma_{\Delta N} = \left(\overline{\Delta N^2}(\rho, h) \right)^{1/2}$ – максимальное значение СКО мелкомасштабных флуктуаций электронной концентрации в неоднородностях ионосферы.

Параметр распределения Райса, который характеризует глубину обших (неселективных) замираний сигнала на входе приемника ССС, определяется через величину СКО флуктуаций фазового фронта выходной волны как [1, 2, 9, 10]

$$\gamma^2 = P_p / P_{\text{фл}} = \left(\exp(\sigma_\varphi^2) - 1 \right)^{-1} = \left(\exp(80,8\pi\sigma_{\Delta N_T} \sec\theta / cf_0)^2 - 1 \right)^{-1}. \quad (2)$$

Полоса когерентности замираний в спутниковом канале (F_k), как и параметр глубины замираний, зависит от несущей частоты, СКО флуктуаций фазового фронта выходной волны и определяется, используя Гауссовский закон распределения, как [1, 2]

$$F_k = \frac{f_0}{\sqrt{\pi}\sigma_\varphi(1+d_1^2/2)^{1/2}} = \frac{f_0^2}{80,8\pi\sqrt{\pi}\sigma_{\Delta N_T} \sec\theta(1+d_1^2/2)^{1/2}}, [\text{Гц}]. \quad (3)$$

Здесь d_1^2 – коэффициент, характеризующий нарастание дифракционных эффектов во фронте волны по мере ее распространения внутри и за ионосферным слоем

$$d_1^2 = (3h_n^2 - 3h_n h_s + h_s^2) c^2 \sec^2\theta / 192\pi^2 f_0^2 l_s^4,$$

где h_n – расстояние от верхней границы ионосферы до точки приема [м].

Согласно (1)–(3) возмущения ионосферы, сопровождаемые увеличением СКО мелкомасштабных флуктуаций ПЭС ионосферы, приводят к увеличению СКО флуктуаций фазового фронта выходной волны $\sigma_\varphi \sim \sigma_{\Delta N_T} \sec\theta / f_0$, которые приводят к уменьшению параметра распределения Райса и полосы когерентности $\gamma^2 \sim (\sigma_\varphi^2)^{-1} \sim (f_0 / \sigma_{\Delta N_T} \sec\theta)^2$; $F_k \sim (\sigma_\varphi)^{-1} \sim f_0 / \sigma_{\Delta N_T} \sec\theta$.

Зависимость коэффициентов энергетических потерь при некогерентной обработке сигналов в каналах связи от степени их ЧСЗ (F/F_k), степени МСИ ($R/F_k = 1/T_s F_k$) описывается выражениями [1, 2]:

$$\eta_q = \left[1 + \frac{1}{2\pi^2} \left(\frac{F}{F_k} \right)^2 \right] \operatorname{erf} \left(\frac{\pi F_k}{F} \right) - \frac{1}{\pi\sqrt{\pi}} \left(\frac{F}{F_k} \right) \left\{ 2 - \exp \left[- \left(\frac{\pi F_k}{F} \right)^2 \right] \right\} \leq 1, \quad (4)$$

$$\eta_m = \frac{1}{2\pi^2} \left(\frac{1}{T_s F_k} \right)^2 \operatorname{erf} (\pi T_s F_k) - \frac{1}{\pi\sqrt{\pi}} \left(\frac{1}{T_s F_k} \right) \exp \left[- (\pi T_s F_k)^2 \right] \geq 0. \quad (5)$$

В соответствии с выражениями (1)–(5) коэффициенты энергетических потерь при обработке сигналов в каналах спутниковой связи зависят от ширины спектра частот (F), скорости передачи (R), несущей частоты (f_0) передаваемого сигнала, СКО мелкомасштабных флуктуаций ПЭС ионосферы ($\sigma_{\Delta N_T}$) на трассе РРВ и угла наклона распространения радиоволн (θ):

$$\{\eta_q; \eta_m\} = \psi(F/F_k; R/F_k) = \psi(F, R, f_0, \sigma_{\Delta N_T}, \theta).$$

Вероятность ошибочного приема сигналов в канале спутниковой связи с одновременным проявлением ЧСЗ, МСИ определяется для случая передачи различных комбинаций трех символов a_{1c} (т.е. 010, 011, 110, 111) как вероятность ошибочного различения центрального символа 1 в виде [4]

$$P_{\text{ош}} = 0,25(P_{111} + P_{110} + P_{011} + P_{010}), \quad (6)$$

где парциальные вероятности ошибки $P_{a_{1c}}$ зависят от парциальных отношений С/Ш на выходе некогерентной схемы обработки $W_{a_{1c}}$:

$$P_{a_{1c}}(W_{a_{1c}}) = \frac{\gamma^2 + 1}{W_{a_{1c}} + 2(\gamma^2 + 1)} \exp \left(- \frac{\gamma^2 W_{a_{1c}}}{W_{a_{1c}} + 2(\gamma^2 + 1)} \right). \quad (7)$$

В выражении (7) параметр Райса определяется согласно (2), а парциальные отношения С/Ш $W_{a_{1c}} = \psi(h^2, \eta_q, \eta_m)$ зависят от отношения С/Ш на входе схемы обработки (h^2) и коэффициентов (4)–(5) энергетических потерь при обработке сигналов из-за ЧСЗ ($\eta_q \leq 1$), МСИ ($\eta_m \geq 0$) согласно выражениям [1, 2]:

$$W_{111} = h^2 \eta_q; W_{110} = W_{011} = \frac{h^2 \eta_q - h^2 \eta_m}{1 + h^2 \eta_m}; W_{010} = \frac{h^2 \eta_q - 2h^2 \eta_m}{1 + 2h^2 \eta_m}; \quad (7a)$$

В соответствии с выражениями (1)–(7) вероятность ошибочного приема сигналов в каналах связи зависит от отношения С/Ш на входе схемы обработки (h^2), ширины спектра частот (F), скорости передачи (R), несущей частоты (f_0) передаваемого сигнала, СКО мелкомасштабных флуктуаций ПЭС ионосферы ($\sigma_{\Delta N_T}$) и угла наклона распространения радиоволн (θ):

$$P_{\text{ош}} = \psi(W_{a_{1c}}, \gamma^2) = \psi(h^2, F/F_k, R/F_k, \gamma^2) = \psi(h^2, F, R, f_0, \sigma_{\Delta N_T}, \theta).$$

В свою очередь, вероятность ошибочного приема сигналов $P_{\text{ош}}$ существенно влияет на пропускную способность канала связи $C=\psi(F, M, P_{\text{ош}})$ с полосой пропускания, соответствующей ширине спектра (F) передаваемого сигнала [4]

$$C = F \left(\log_2 M + P_{\text{ош}} \log_2 (P_{\text{ош}} / M - 1) + (1 - P_{\text{ош}}) \log_2 (1 - P_{\text{ош}}) \right). \quad (8)$$

В соответствии с зависимостями (2) $\gamma^2 = \psi(f_0, \sigma_{\Delta N_T}, \theta)$, (6, 7) $P_{\text{ош}} = \psi(h^2, \gamma^2)$ и (8) $C = \psi(F, M, P_{\text{ош}})$ пропускная способность для М-уровневого симметричного спутникового канала связи с ЧСЗ и МСИ определяется согласно выражению

$$C = F \left(\log_2 M + P_{\text{ош}} \left(h^2, F, R, f_0, M, \sigma_{\Delta N_T}, \theta \right) \log_2 \left(P_{\text{ош}} \left(h^2, F, R, f_0, M, \sigma_{\Delta N_T}, \theta \right) / M - 1 \right) + \right. \\ \left. + \left(1 - P_{\text{ош}} \left(h^2, F, R, f_0, M, \sigma_{\Delta N_T}, \theta \right) \right) \log_2 \left(1 - P_{\text{ош}} \left(h^2, F, R, f_0, M, \sigma_{\Delta N_T}, \theta \right) \right) \right) \quad (8a)$$

В частном случае, отсутствия ЧСЗ, МСИ в канале спутниковой связи ($F/F_k \ll 1$, $\eta_c = 1$, $\eta_m = 0$, $W_{\text{длс}} = h^2$) выражение (7) сводится к известному виду для случая райсовских замираний [1, 2].

$$P_{\text{ош}} = P_{\text{ош}}(h^2, \gamma^2) = \frac{\gamma^2 + 1}{h^2 + 2(\gamma^2 + 1)} \exp \left(-\frac{\gamma^2 h^2}{h^2 + 2(\gamma^2 + 1)} \right). \quad (96)$$

В традиционно рассматриваемом для канала спутниковой связи случае отсутствия замираний принимаемого сигнала выражение (96) сводится к известному [7, 8] виду для некогерентного приема двоичных сигналов с частотной манипуляцией (BFSK):

$$P_{\text{ош}}(h^2) = 0,5 \exp(-0,5h^2) \quad (9в)$$

При подстановке (9в) в выражение (8) можно определить пропускную способность спутникового канала связи без замираний $C_{\text{бз}}$ и относительное уменьшение пропускной способности спутникового канала связи с ЧСЗ, МСИ по сравнению с каналом без замираний:

$$\Delta C(h^2, F, R, f_0, M, \sigma_{\Delta N_T}, \theta) = C(h^2, F, R, f_0, M, \sigma_{\Delta N_T}, \theta) / C_{\text{бз}}(h^2, F, R, f_0, M). \quad (10)$$

Конкретизируем параметры передаваемых сигналов ССС и ионосферы ($f_0, F, R, M, \theta, \sigma_{\Delta N_T}$):

- несущая частота $f_0 = 387$ МГц;
- ширина спектра $F = 100$ кГц;
- скорость передачи $R = 100$ кбит/с;
- кратность модуляции $M = 2$;
- угол наклона распространения радиоволн $\theta = 60^\circ$;
- наклонное СКО флуктуаций ПЭС на трассе распространения радиоволн изменяется в пределах от $\sigma_{\Delta N_T} =$

$2,488 \cdot 10^{16}$ до $\sigma_{\Delta N_T} = 5,488 \cdot 10^{17}$ таким образом, чтобы полоса когерентности канала спутниковой связи уменьшалась в пределах от $F_k = 4,08$ МГц ($F/F_k = 0,025$) до $F_k = 181,9$ кГц ($F/F_k = 0,55$). Такое изменение соответствует искусственным возмущениям ионосферы. Заметим, что фактические значения наклонного СКО мелкомасштабных флуктуаций ПЭС ионосферы могут быть получены комплексом прогнозирования помехоустойчивости ССС на основе ГНСС-зондирования ионосферы [5, 8, 11].

Подстановка указанных выше параметров передаваемых сигналов ССС и ионосферы ($f_0, F, R, \theta, \sigma_{\Delta N_T}$) в выражения (1)-(9в) позволяет определить (рисунок 1) зависимость $\Delta C(h^2, F, R, f_0, M, \sigma_{\Delta N_T}, \theta)$ (10) относительной пропускной способности канала спутниковой связи с ЧСЗ и МСИ от отношения F/F_k , при отношениях C/Π $h^2 = 7$ дБ (график 1), $h^2 = 15$ дБ (график 2), $h^2 = 23$ дБ (график 3).

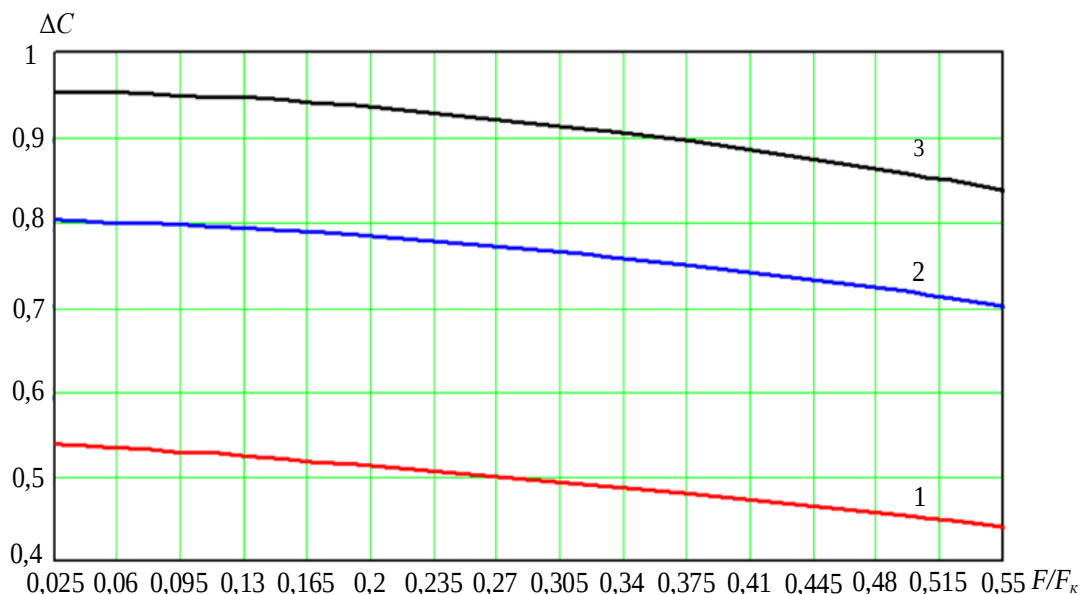


Рисунок 1. Относительная пропускная способность ΔC канала спутниковой связи с частотно-селективными замираниями и межсимвольной интерференцией в зависимости от увеличения отношения F/F_k при несущей частоте $f_0=387$ МГц, отношении C/Π 1. $h^2=7$ дБ; 2. $h^2=15$ дБ; 3. $h^2=23$ дБ

Анализ рисунка 1 показывает, что на низкой несущей частоте ($f_0=387$ МГц) в условиях искусственных возмущений ионосферы на графиках 1, 2 и 3 появляется снижение по сравнению с величиной $\Delta C = 1$ относительной пропускной способности канала спутниковой связи из-за появления ЧСЗ и МСИ принимаемых сигналов. Заметим, что $F/F_k=0,025$ соответствует случаю релейских замираний в канале ($\gamma^2=0$). Если в качестве критерия допустимого снижения относительной пропускной способности канала спутниковой связи из-за ЧСЗ и МСИ принять величину:

- 5% при $h^2=7$ дБ (т.е. с $\Delta C = 0,54$ до $\Delta C = 0,49$), уточненное условие отсутствия ЧСЗ и МСИ в канале спутниковой связи в виде: $F/F_k \leq 0,32$, или $F \leq 0,32F_k$;

- при $h^2=15$ дБ (т.е. с $\Delta C = 0,8$ до $\Delta C = 0,75$), уточненное условие отсутствия ЧСЗ и МСИ в канале спутниковой связи в виде: $F/F_k \leq 0,37$, или $F \leq 0,37F_k$;

- при $h^2=23$ дБ (т.е. с $\Delta C = 0,95$ до $\Delta C = 0,9$), уточненное условие отсутствия ЧСЗ и МСИ в канале спутниковой связи в виде: $F/F_k \leq 0,33$, или $F \leq 0,33F_k$;

- 10% при $h^2=7$ дБ (т.е. с $\Delta C = 0,54$ до $\Delta C = 0,44$), уточненное условие отсутствия ЧСЗ и МСИ в канале спутниковой связи в виде: $F/F_k \leq 0,55$, или $F \leq 0,55F_k$;

- при $h^2=15$ дБ (т.е. с $\Delta C = 0,8$ до $\Delta C = 0,7$), уточненное условие отсутствия ЧСЗ и МСИ в канале спутниковой связи в виде: $F/F_k \leq 0,55$, или $F \leq 0,55F_k$;

- при $h^2=23$ дБ (т.е. с $\Delta C = 0,95$ до $\Delta C = 0,85$), уточненное условие отсутствия ЧСЗ и МСИ в канале спутниковой связи в виде: $F/F_k \leq 0,5$, или $F \leq 0,5F_k$;

Таким образом, обеспечить выполнение условий отсутствия ЧСЗ и МСИ в канале спутниковой связи возможно за счет уменьшения ширины спектра передаваемого сигнала F по результатам предварительного расчета согласно (3) полосы когерентности замираний $F_k = \psi(f_0, \sigma_{\Delta N_T}(\theta))$ в спутниковом канале связи на основе известных значений несущей частоты сигнала и угла наклона его распространения и результатов мониторинга СКО мелкомасштабных флуктуаций ПЭС ионосферы.

Элементами новизны представленного решения является использование параметра ионосферы (СКО ПЭС) при оценке пропускной способности канала спутниковой связи с ЧСЗ и МСИ, для обеспечения выполнения уточненного условия отсутствия ЧСЗ и МСИ в канале. Параметр ионосферы СКО ПЭС может быть получен комплексом прогнозирования помехоустойчивости систем спутниковой связи на основе ГНСС-зондирования ионосферы [5, 8, 11].

Литература

1. Маслов О. Н., Пашинцев В. П. Модели трансionoсферных радиоканалов и помехоустойчивость систем космической связи // Инфокоммуникационные технологии (приложение к журналу). 2006. № 4. 357 с.
2. Пашинцев В.П. Модели трансionoсферных радиоканалов и помехоустойчивость систем космической связи. Монография. – Москва; Вологда: Инфра-Инженерия, 2026. – 212 с.
3. Иванов Д.В., Иванов В.А., Рябова Н.В., Кислицын А.А. Создание комплексной модели чирпинг-эффекта трансionoсферного широкополосного радиоканала. Часть 1. Радиотехнический подход // Радиотехника. 2025. Т. 89. № 12. С. 147–159. DOI: <https://doi.org/10.18127/j00338486-202512-16>
4. Пашинцев В. П., Диптан П. А., Белоконь Д. А. Методика прогнозирования пропускной способности канала спутниковой связи при мелкомасштабных возмущениях ионосферы, возникновении частотно-селективных замираний и межсимвольной интерференции // Системы управления, связи и безопасности. 2025. № 1. С. 156-186. DOI: 10.24412/2410-9916-2025-1-156-186
5. Пашинцев В.П., Коваль С. А., Скорик А. Д., Диптан П. А. Комплекс оценки полосы пропускания трансionoсферного канала связи на основе результатов GPS–мониторинга ионосферы. // В сборнике: Распространение радиоволн. Сборник докладов XXVIII Всероссийской открытой научной конференции. Йошкар-Ола, 2023. С. 164–167.
6. Пашинцев В.П., Копытов В. В., Михайлов Д. А., Бойченко И. А., Диптан П. А. Прогнозирование помехоустойчивости спутниковой системы Коспас-Сарсат на основе результатов GPS-мониторинга мелкомасштабных возмущений ионосферы // Журнал радиоэлектроники. 2024. № 12. С. 1-44. DOI: [10.30898/1684-1719.2024.12.1](https://doi.org/10.30898/1684-1719.2024.12.1)
7. Пашинцев В. П., Диптан П. А., Гринев Е. М., Белоконь Д. А., Киселев Н. В. Пропускная способность спутникового канала связи с частотно-селективными замираниями и межсимвольной интерференцией. // В сборнике: Радиоэлектронные устройства и системы для инфокоммуникационных технологий (РЭУС-ИТ 2024). Доклады всероссийской конференции, посвященной «Дню Радио». Москва, 2024. С. 208-213
8. Пашинцев В.П., Песков М.В., Михайлов Д.А., Диптан П.А. Прогнозирование помехоустойчивости системы спутниковой связи R-диапазона при сильных возмущениях ионосферы // Журнал радиоэлектроники. – 2025. – №. 12. <https://doi.org/10.30898/16841719.2025.12.7>
9.] Финк Л. М. Теория передачи дискретных сообщений. М.: Издательство «Советское радио», 1970. 728 с.
10. Кловский Д. Д. Передача дискретных сообщений по радиоканалам. М.: Издательство «Радио и связь», 1982. 304 с.
11. Pashintsev V. P., Peskov M. V., Senokosov M. A., Mikhailov D. A., Skorik A. D. A system for measuring the scintillation index based on the results of monitoring of small-scale fluctuations in the total electron content of the ionosphere // GPS Solutions. 2024. Vol. 28. No. 1. P. 1–14. DOI: 10.1007/s10291-023-01550-1.

REFINED CONDITION OF ABSENCE OF FREQUENCY-SELECTIVE FADING AND INTERSYMBOL INTERFERENCE IN SATELLITE COMMUNICATION CHANNEL AT IONOSPHERE DISTURBANCES

postgrad. Diptan P. A.

North-Caucasus Federal University

. The refined conditions of absence of frequency-selective fading and intersymbol interference in a satellite communication channel with a given spectrum width F are obtained with narrowing of the coherence band F_k of fading under conditions of artificial disturbances of the ionosphere and realisation of different signal-to-noise ratio at the input of the receiver (7dB, 15dB and 23dB) according to the criterion of reducing throughput. It is shown that when implementing the signal-to-noise ratio at the receiver input of 7-15 dB, the throughput of the satellite communication channel decreases by 10% (relative to the case of Rayleigh fading) when $F \leq 0.55F_k$



СЕКЦИЯ № 6.

ЗАЩИТА ИНФОРМАЦИИ, В Т.Ч. КОДИРОВАНИЕ, И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ.

МЕТОДИКА РАСЧЕТА ЗАТУХАНИЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

проф. Хорев А.А., студ. Борисов Р.М.

Национальный исследовательский университет «МИЭТ»

В статье представлены методики расчета затуханий побочных электромагнитных излучений (ПЭМИ) средств вычислительной техники (СВТ), основанных на теории Д.Максвелла об электромагнитных волнах и на предположении, что в ближней зоне напряженность поля падает обратно пропорционально кубу расстояния ($E \sim 1/r^3$), в средней зоне – обратно пропорционально квадрату расстояния ($E \sim 1/r^2$), а в дальней зоне – обратно пропорционально расстоянию ($E \sim 1/r$). Проведена сравнительная оценка результатов расчетов затухания ПЭМИ по разработанным методикам.

Введение

Одним из показателей оценки возможности технических средств разведки (ТСР) по перехвату побочных электромагнитных излучений (ПЭМИ) средств вычислительной техники (СВТ) является опасная зона R2, под которой понимается пространство, в пределах которого отношение сигнал/шум на входе приемного устройства ТСР (q) превышает установленное пороговое значение (δ) [1].

Оценка опасной зоны R2 проводится инструментально-расчетным методом, предполагающим измерение напряженности поля ПЭМИ СВТ на расстоянии 1 м от СВТ, расчет затухания ПЭМИ на трассе СВТ – ТСР и расчет отношения сигнал/шум на входе приемного устройства ТСР с учетом затухания ПЭМИ [1]. За значение опасной зоны R2 принимается максимальное расстояние (r), при котором $q \geq \delta$.

Целью исследований является разработки методики расчета затухания ПЭМИ.

1. Методические подходы к расчету затухания ПЭМИ

Для расчета затухания ПЭМИ в основном используются классический и упрощенный подходы.

Классический подход основан на теории Джеймса Максвелла об электромагнитных волнах.

В соответствии с этой теорией электромагнитные волны (ЭМВ) могут быть продольными и поперечными. Если электромагнитная волна распространяется в однородной и изотропной среде, не обладающей сегнетоэлектрическими и ферромагнитными свойствами, а также не проводящей электрический ток, так что векторы напряженности электрического ($\vec{E}$), магнитного ($\vec{H}$) и единичный вектор направления распространения волны ($\vec{n}$) взаимно перпендикулярны, то в указанных условиях электромагнитные волны являются поперечными волнами.

Полагая, что напряженность электрического поля поперечных электромагнитных волн (E_n), значительно больше напряженности электрического поля продольных электромагнитных волн (E_{nd}). Тогда, можно полагать, что $E \approx E_n$, и затухание ПЭМИ на частоте f на расстоянии r от источника излучения $V_{f,r}$ можно рассчитать по формуле [2]:

$$V_{f,r} \approx 1/K_{n,f}(r); \quad (1)$$

$$K_{n,f}(r) = \frac{r_0^3}{r^3} \sqrt{\frac{k^4 r^4 - k^2 r^2 + 1}{k^4 r_0^4 - k^2 r_0^2 + 1}}, \quad (2)$$

где $K_{n,f}(r)$ – коэффициент ослабления поперечной компоненты электрической составляющей электромагнитного поля на частоте f и на расстоянии r от источника излучения;

$$k = \frac{2\pi}{\lambda} \text{ – волновое число;}$$

λ – длина волны излучения, м;

r_o – опорное расстояние (расстояние от источника излучения, на котором проводилось измерение напряженности поля), м;

r – расстояние от источника излучения, м.

Полагая $r_o = 1$ м, формулу (2) запишем в виде:

$$K_{n.f}(r) = \frac{1}{r^3} \sqrt{\frac{k^4 r^4 - k^2 r^2 + 1}{k^4 - k^2 + 1}}. \quad (3)$$

Упрощенный подход основан на предположении, что в ближней зоне напряженность поля падает обратно пропорционально кубу расстояния ($E \sim 1/r^3$), в средней зоне – обратно пропорционально квадрату расстояния ($E \sim 1/r^2$), а в дальней зоне – обратно пропорционально расстоянию ($E \sim 1/r$).

Граница ближней зоны ($R_{бз}$) рассчитывается по формуле [2]

$$R_{бз} = \frac{\lambda}{2\pi} = \frac{300}{2\pi \cdot f}, \quad (4)$$

где f – частота излучения, МГц.

Граница дальней зоны связана с длиной волны соотношением:

$$R_{дз} = Z \cdot \lambda, \quad (5)$$

где Z – коэффициент, который по разным источникам может принимать значения от 3 до 10.

Средняя зона является промежуточной областью между ближней и дальней зонами.

Учитывая, что $r_o = 1$ м формулы, расчет затухания электромагнитных волн на частоте f на расстоянии r от источника излучения $V_{f,r}$ можно провести по формулам:

а) для частот $f \leq 47,75$ МГц:

$$V_f(r) = \begin{cases} r^3, & \text{если } r \leq R_{бз}; \\ (R_{бз})^3 \cdot \left(\frac{r}{R_{бз}}\right)^2, & \text{если } R_{бз} < r \leq R_{дз}; \\ (R_{бз})^3 \cdot \left(\frac{R_{дз}}{R_{бз}}\right)^2 \cdot \left(\frac{r}{R_{дз}}\right), & \text{если } r > R_{дз}; \end{cases} \quad (6)$$

б) для частот в диапазоне $47,75 \text{ МГц} < f \leq 300 \cdot Z \text{ МГц}$:

$$V_f(r) = \begin{cases} r^2 & \text{если } r \leq R_{дз}; \\ (R_{дз})^2 \cdot \left(\frac{r}{R_{дз}}\right), & \text{если } r > R_{дз}; \end{cases} \quad (7)$$

в) для частот $f > 300 \cdot Z \text{ МГц}$:

$$V_f(r) = r. \quad (8)$$

При оценке затухания ПЭМИ необходимо рассчитать среднее затухание в частотном интервале ΔF_j :

$$\bar{V}_r(\Delta F_j) \approx \sqrt{\frac{\sum_{i=1}^{i=N_j} [(V_{f_i,r})^2 \cdot \Delta F_i]}{\Delta F_j}}, \quad (9)$$

где $\bar{V}_r(\Delta F_j)$ – среднее затухание в частотном интервале ΔF_j ;

$f_{j,n}$ – нижняя частота частотного интервала ΔF_j , МГц;

$f_{j,v}$ – верхняя частота частотного интервала ΔF_j , МГц;

$f_i = f_{j,n} + (i - 1) \cdot \Delta F_i$ – i -я частота излучения, для которой рассчитывается затухание, МГц;

i – номер частоты излучения в j -м частотном интервале, для которой рассчитывается затухание, МГц;

$f_{N_j} = f_{j,v} - \Delta F_{N_j}$ – конечная частота в j -м частотном интервале, для которой рассчитывается затухание, МГц;

ΔF_i – шаг смещения частоты при расчете затухания ПЭМИ на i -м шаге, МГц;

N_j – количество точек расчета коэффициента затухания ПЭМИ в частотном интервале ΔF_j .

Для расчета затухания ПЭМИ в дБ воспользуемся формулами:

$$V_f^*(r) = 20 \lg V_f(r). \quad (10)$$

$$\bar{V}_f^*(\Delta F_j) = 20 \lg \bar{V}_r(\Delta F_j). \quad (11)$$

2. Сравнительная оценка результатов расчетов затухания ПЭМИ по классической и упрощенной методикам

Для расчета затухания ПЭМИ на языке программирования Python было разработано специальное программное обеспечение (СПО).

Исследования проходили в три этапа.

На первом этапе были рассчитаны графики зависимости затухания ЭМИ ($V_f(r)$) от частоты (f) по классической и упрощенной методикам. При этом в упрощенной методике расчет проводился для трех значений $R_{дз}$: $R_{дз} = 3\lambda$; $R_{дз} = 6\lambda$; $R_{дз} = 10\lambda$.

Сравнительный анализ полученных зависимостей показал, что наибольшее сходство рассчитанных значений затуханий ЭМИ по классической и упрощенной методикам наблюдается при $R_{дз} = 3\lambda$ (рисунок 1).

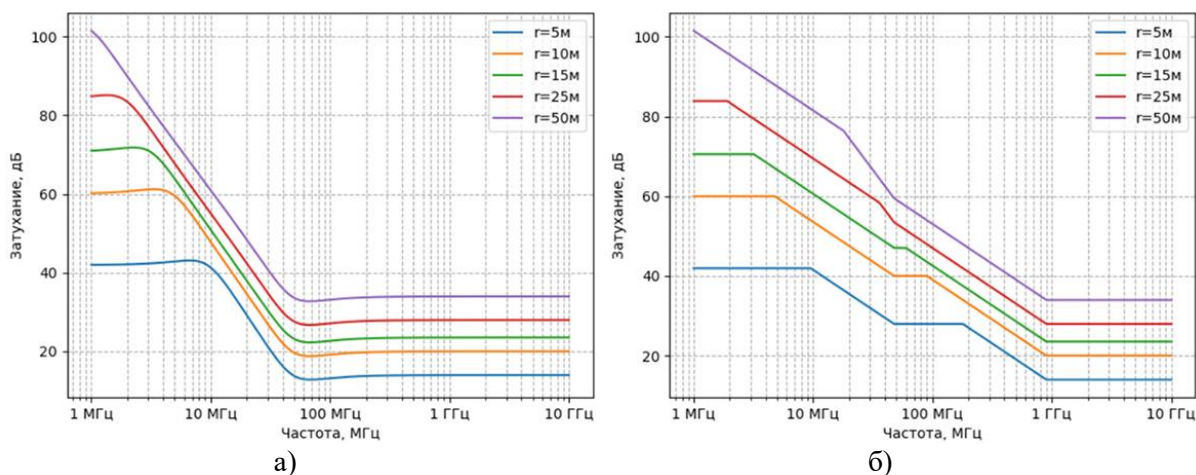


Рисунок 1 - Графики зависимости затухания ЭМИ ($V_f(r)$) от частоты (f) по классической методике (а) и упрощенной методике при $R_{дз} = 3\lambda$ (б)

На втором этапе были рассчитаны графики зависимости среднего затухания ПЭМИ в частотных интервалах $\bar{V}_f(\Delta F_j)$ от расстояния до СВТ (r) по классической и упрощенной методикам (при $R_{дз} = 3\lambda$). При этом шаг измерения затухания ПЭМИ в частотных интервалах был постоянен и составлял $\Delta F_i = 100$ Гц.

В качестве режима работы СВТ был выбран режим вывода информации на экран монитора с параметрами: разрешение 1920×1080 пикселей, частота обновления кадров – 67,5 Гц, пиксельная частота – $F_n = 148,5$ МГц.

Для расчетов были выбраны 16 частотных интервалов ПЭМИ, границы которых рассчитаны в соответствии с методикой, приведенной в [1].

Результаты расчетов среднего затухания ПЭМИ в частотных интервалах приведены на рисунках 2–5.

Учитывая, что в диапазоне частот от 9 кГц до 10 МГц практически отсутствуют информативные составляющие ПЭМИ видеосистем СВТ, а затухание на дальностях более 10 м превышает 60 дБ, для 1-го частотного интервала расчет среднего затухания проведен в диапазоне частот от 10 МГц до 148,5 МГц.

В таблице 1 приведены разности результатов расчетов по классической и упрощенной методикам:

$$\Delta \bar{V}_f^*(\Delta F_j) = \bar{V}_f^*(\Delta F_j)_{\text{кл}} - \bar{V}_f^*(\Delta F_j)_{\text{упр}}. \quad (12)$$

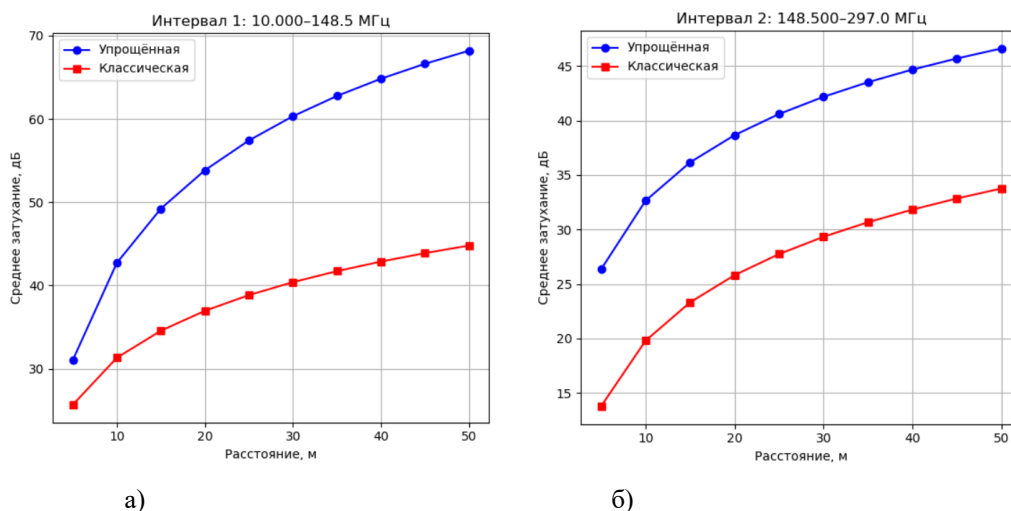


Рисунок 2 – Графики зависимости среднего затухания ПЭМИ в частотных интервалах $\bar{V}_r(\Delta F_j)$ от расстояния до СВТ, рассчитанные по классической и упрощенной методикам (при $R_{дз} = 3\lambda$) для 1-го частотного интервала (а) и для 2-го частотного интервала (б)

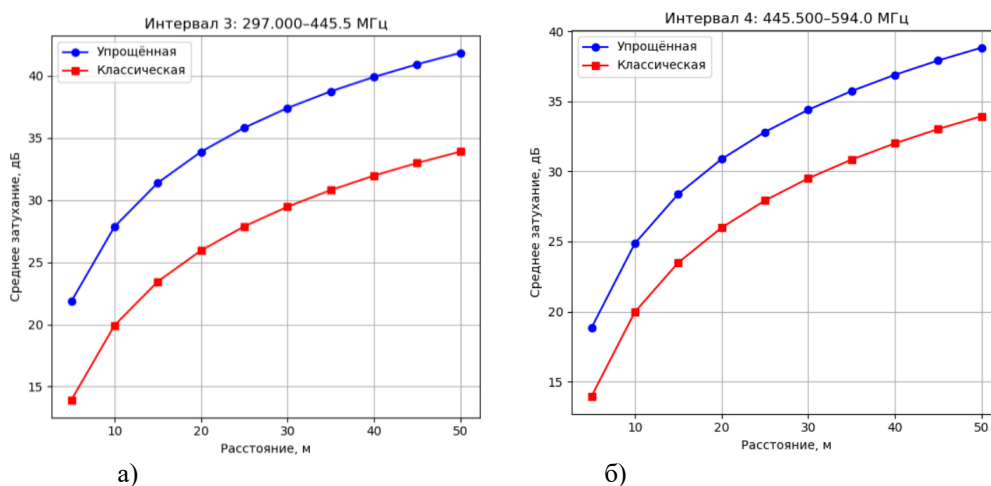


Рисунок 3 – Графики зависимости среднего затухания ПЭМИ в частотных интервалах $\bar{V}_r(\Delta F_j)$ от расстояния до СВТ, рассчитанные по классической и упрощенной методикам (при $R_{дз} = 3\lambda$) для 3-го частотного интервала (а) и для 4-го частотного интервала (б)

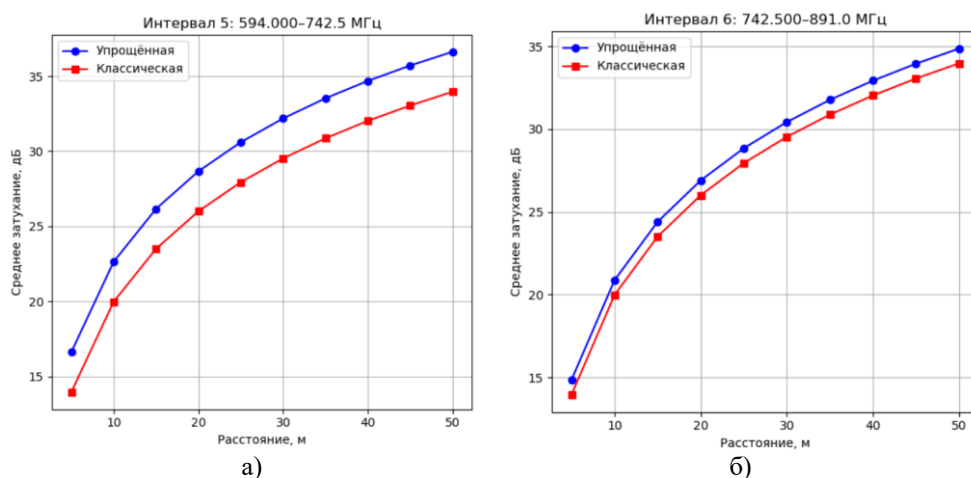


Рисунок 4 – Графики зависимости среднего затухания ПЭМИ в частотных интервалах $\bar{V}_r(\Delta F_j)$ от расстояния до СВТ, рассчитанные по классической и упрощенной методикам (при $R_{дз} = 3\lambda$) для 5-го частотного интервала (а) и для 6-го частотного интервала (б)

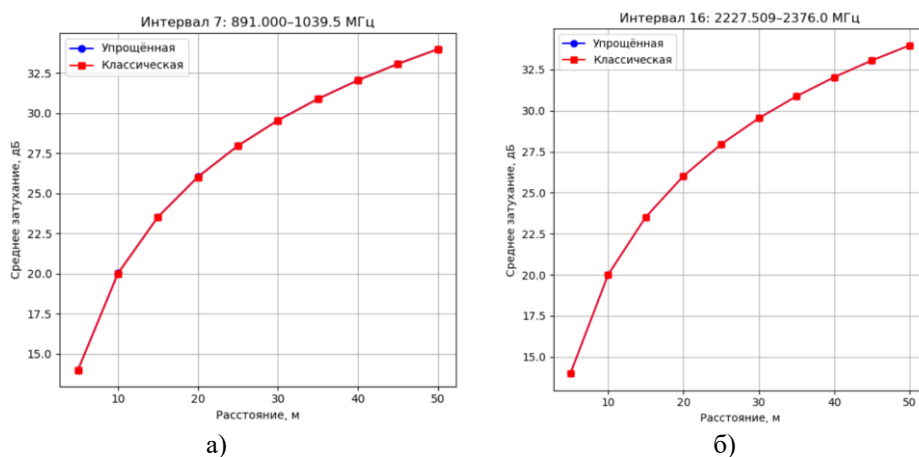


Рисунок 5 – Графики зависимости среднего затухания ПЭМИ в частотных интервалах $\bar{V}_r(\Delta F_j)$ от расстояния до СВТ, рассчитанные по классической и упрощенной методикам (при $R_{дз} = 3\lambda$) для 7-го частотного интервала (а) и для 16-го частотного интервала (б)

Таблица 1

Разность результатов расчетов среднего затухания ПЭМИ по классической и упрощенной методикам $\bar{\Delta V}_f^*(\Delta F_j)$

Номер интервала, j	$\bar{\Delta V}_f^*(\Delta F_j)$, дБ		
	Расстояние 10 м	Расстояние 20 м	Расстояние свыше 30 м
1	– 11,4 дБ	– 16,9 дБ	– 23,4 дБ
2	– 12,8 дБ	– 12,8 дБ	– 12,8 дБ
3	– 7,9 дБ	– 7,9 дБ	– 7,9 дБ
4	– 4,9 дБ	– 4,9 дБ	– 4,9 дБ
5	– 2,6 дБ	– 2,6 дБ	– 2,6 дБ
6	– 0,9 дБ	– 0,9 дБ	– 0,9 дБ
7 – 16	0 дБ	0 дБ	0 дБ

Заключение

Анализ графиков, приведенных на рисунках 2 – 5, и данных, представленных в таблице 1, показал, что: с 1-го до 6-го частотного интервалов затухание, рассчитанное по упрощенной методике, выше, чем рассчитанное по классической методике, что приводит занижению опасной зоны R2;

разность результатов расчетов по классической и упрощенной методикам в 1-м частотном интервале на дальностях свыше 30 м составляет $\sim -23,4$ дБ;

начиная со 2-го частотного интервала разность результатов расчетов по классической и упрощенной методикам существенно уменьшается;

начиная с 7 частотного интервала (на частотах более 900 МГц) результаты расчетов по классической и упрощенной методикам совпадают.

Следовательно, упрощенную методику можно использовать для расчета среднего затухания ПЭМИ $\bar{\Delta V}_f^*(\Delta F_j)$ только на частотах свыше 900 МГц.

Литература

- Хорев А.А. Некоторые подходы к оценке возможностей перехвата побочных электромагнитных излучений средств вычислительной техники, использующих цифровые интерфейсы// Вестник УрФО «Безопасность в информационной сфере». – Челябинск, УрФО. – 2022. - № 3(45) – С. 5 – 16
ISSN: 2225-5435

2. Авдеев В.Б., Катруша А.Н. Оценка уровня побочного электромагнитного излучения на границе контролируемой зоны с учетом продольной компоненты поля//Специальная техника. – М.: 2014.- № 1. С. 28-34.

METHOD FOR CALCULATING THE ATTENUATION OF PARTIAL ELECTROMAGNETIC RADIATION OF COMPUTER EQUIPMENT

prof. Horev A.A., stud. Borisov R.M.

National Research University of Electronic Technology

The article presents methods for calculating the attenuation of electromagnetic side effects (EMI) of computer technology (CBT), based on D. Maxwell's theory of electromagnetic waves and on the assumption that in the near zone the field strength decreases inversely proportional to the cube of the distance ($E \sim 1/r^3$), in the middle zone – inversely proportional to the square of the distance ($E \sim 1/r^2$), and in the far zone – is inversely proportional to the distance ($E \sim 1/r$). A comparative assessment of the results of EMR attenuation calculations using the developed methods was carried out.



ОБОСНОВАНИЕ РАЦИОНАЛЬНОГО ШАГА ИЗМЕНЕНИЯ ЧАСТОТЫ ПРИ РАСЧЕТЕ ЗАТУХАНИЯ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

проф. Хорев А.А., студ. Борисов Р.М.

Национальный исследовательский университет «МИЭТ»

В статье проведено обоснование рационального шага изменения частоты при расчете затухания побочных электромагнитных излучений средств вычислительной техники, проведенных по классической методике, основанной на теории Д. Максвелла, и по упрощенной методике, основанной на предположении, что в ближней зоне напряженность поля падает обратно пропорционально кубу расстояния ($E \sim 1/r^3$), в средней зоне – обратно пропорционально квадрату расстояния ($E \sim 1/r^2$), а в дальней зоне – обратно пропорционально расстоянию ($E \sim 1/r$). В результате расчетов установлено, что минимальный шаг изменения частоты должен составлять не более 30 - 70 МГц.

[2]

Одним из показателей оценки возможности технических средств разведки (ТСР) по перехвату побочных электромагнитных излучений (ПЭМИ) средств вычислительной техники (СВТ) является опасная зона R2, под которой понимается пространство, в пределах которого отношение сигнал/шум на входе приемного устройства ТСР (q) превышает установленное пороговое значение (δ) [1].

Оценка опасной зоны R2 проводится инструментально-расчетным методом, предполагающим измерение напряженности поля ПЭМИ СВТ на расстоянии 1 м от СВТ, расчет затухания ПЭМИ на трассе СВТ – ТСР и расчет отношения сигнал/шум на входе приемного устройства ТСР с учетом затухания ПЭМИ [1]. За значение опасной зоны R2 принимается максимальное расстояние, при котором $q \geq \delta$.

Для расчета затухания ПЭМИ в основном используются классический и упрощенный подходы [2].

В большинстве случаев расчет затухания ПЭМИ проводится с использованием специального программного обеспечения (СПО) и занимает несколько минут.

Однако не всегда есть возможность проводить расчеты с использованием СПО, в ряде случаев возникает необходимость провести расчеты затухания ПЭМИ с использованием калькулятора.

Целью исследований является обоснование рационального шага изменения частоты при расчете затухания ПЭМИ с использованием калькулятора.

При равномерном шаге изменения частоты (ΔF) среднее затухание в частотном интервале ΔF_j рассчитывается по формуле:

$$\bar{V}_r(\Delta F_j, \Delta F) \approx \sqrt{\frac{\sum_{i=1}^{N-1} [(V_{f_i, r})^2]}{N}}, \quad (1)$$

где $V_{f, r}$ – затухание электромагнитных волн на частоте f на расстоянии r от источника излучения;

$f_i = f_{j, n} + (i - 1) \cdot \Delta F$ – i -я частота излучения, для которой рассчитывается затухание, МГц;

i – номер частоты излучения в j -м частотном интервале, для которой рассчитывается затухание, МГц;

$f_N = f_{j, b}$ – конечная частота в j -м частотном интервале, для которой рассчитывается затухание, МГц;

$f_{j, n}$ – нижняя частота частотного интервала ΔF_j , МГц;

$f_{j, b}$ – верхняя частота частотного интервала ΔF_j , МГц;

$\Delta F = \Delta F_j / (N - 1) = (f_{j, b} - f_{j, n}) / (N - 1)$ – шаг смещения (изменения) частоты при расчете затухания ПЭМИ, МГц.

N – количество частот для расчета коэффициента затухания ПЭМИ в частотном интервале ΔF_j .

При проведении исследований в качестве режима работы СВТ был выбран режим вывода информации на экран монитора с параметрами: разрешение 1920×1080 пикселей, частота обновления кадров – 67,5 Гц, пиксельная частота – $F_n = 148,5$ МГц.

Для расчетов затухания ПЭМИ были выбраны 16-ть частотных интервалов ПЭМИ, границы которых рассчитаны в соответствии с методикой, приведенной в [1].

С использованием СПО был проведен расчет среднего затухания в 16 частотных интервалах $\bar{V}_r(\Delta F_j, \Delta F)$ по классической и упрощенной методикам [2] для различного количества частот в частотном интервале, на которых рассчитывается затухание ПЭМИ: $N = 1\,485\,000$ ($\Delta F \approx 100$ Гц), $N = 148\,500$ ($\Delta F \approx 1$ кГц), $N = 14$

850 ($\Delta F \approx 10$ кГц), $N = 1\,485$ ($\Delta F \approx 100$ кГц), $N = 148$ ($\Delta F \approx 1$ МГц), $N = 15$ ($\Delta F \approx 10,6$ МГц), $N = 6$ ($\Delta F \approx 29,7$ МГц), $N = 3$ ($\Delta F \approx 74,25$ МГц) и $N = 1$ (для центральной частоты частотного интервала).

Учитывая, что в диапазоне частот от 9 кГц до 10 МГц практически отсутствуют информативные составляющие ПЭМИ видеосистем СВТ, а затухание на дальностях более 10 м превышает 60 дБ, для 1-го частотного интервала расчет среднего затухания проведен в диапазоне частот от 10 МГц до 148,5 МГц.

Далее, для каждого частотного интервала был проведен расчет отклонения величины затухания ПЭМИ в зависимости от шага изменения частоты ΔF_N относительно шага $\Delta F_{N=\max}=100$ Гц по формуле:

$$\overline{\Delta V}_r(\Delta F_j, \Delta F_N) = \overline{\Delta V}_r(\Delta F_j, \Delta F_{N=\max}) - \overline{\Delta V}_r(\Delta F_j, \Delta F_N), \quad (2)$$

где $\overline{\Delta V}_r(\Delta F_j, \Delta F_N)$ – среднее затухание ПЭМИ в j -м частотном интервале на дальности r от источника излучения, дБ;

ΔF_N – шаг смещения (изменения) частоты в j -м частотном интервале, МГц;

N – количество частот в j -м частотном интервале на которых рассчитывается затухание ПЭМИ;

$\Delta F_{N=\max}$ – шаг смещения (изменения) частоты в j -м частотном интервале при максимальном количестве частот $N_{\max} = 1\,485\,000$, на которых рассчитывается затухание ПЭМИ ($\Delta F_{N=\max} = 10^{-5}$ МГц), МГц.

Анализ полученных результатов расчетов $\overline{V}_r(\Delta F_j, \Delta F)$ по классической методике показал, что:

для 1-го частотного интервала (рисунки 1; 2 и таблица 1) существенные отличия величины затухания ПЭМИ от значений, рассчитанных для шага $\Delta F = 100$ Гц, начинаются с увеличением шага более 1 МГц (148 точек на интервал). Ошибка менее 0,5 дБ наблюдается при шаге изменения частоты менее $\Delta F < 1$ МГц ($N > 148$);

начиная со 2-го частотного интервала шаг изменения частоты практически не влияет на ошибку расчета величины затухания. Даже, при расчете затухания на одной центральной частоте частотного интервала ΔF_j ошибка не превышает 0,02 дБ.

Анализ полученных результатов по упрощенной методике показал, что:

для 1-го частотного интервала существенные отличия величины затухания ПЭМИ от значений, рассчитанных для шага $\Delta F = 100$ Гц, начинаются с увеличением шага $\Delta F \geq 100$ кГц ($N \leq 1480$). Ошибка менее 0,5 дБ наблюдается при шаге изменения частоты $\Delta F < 5$ МГц ($N < 30$) (рисунок 3 и таблица 2);

для 2-го частотного интервала шаг изменения частоты практически не влияет на ошибку расчета величины затухания при шаге изменения частоты $\Delta F \leq 10$ МГц ($N \geq 15$). Ошибка менее 0,5 дБ наблюдается даже при расчете затухания на одной центральной частоте частотного интервала ΔF_j (рисунок 4 и таблица 2);

для 3-го частотного интервала шаг изменения частоты практически не влияет на ошибку расчета величины затухания при шаге изменения частоты $\Delta F \leq 30$ МГц ($N \geq 6$). При расчете затухания на одной центральной частоте частотного интервала ΔF_j ошибка менее 0,2 дБ (рисунок 5 и таблицу 2);

начиная с 4-го частотного интервала шаг изменения частоты незначительно влияет на ошибку расчета величины затухания (см. таблицу 2).

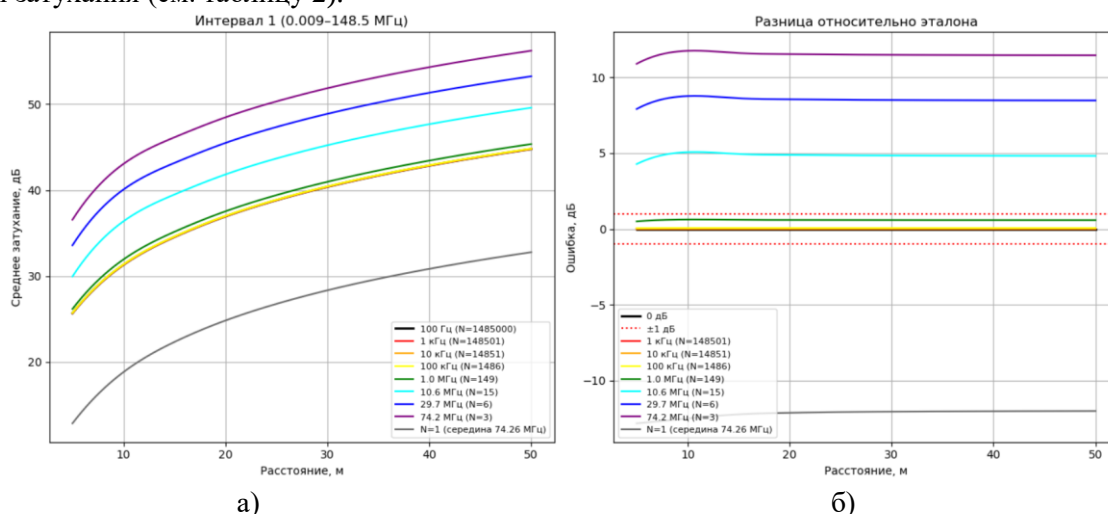


Рисунок 1 – Графики, рассчитанные по классической методике для 1-го частотного интервала для различного шага изменения частоты в зависимости от расстояния до СВТ: среднего затухания ПЭМИ $\overline{V}_r(\Delta F_j)$ (а) и ошибок измерения затухания (б)

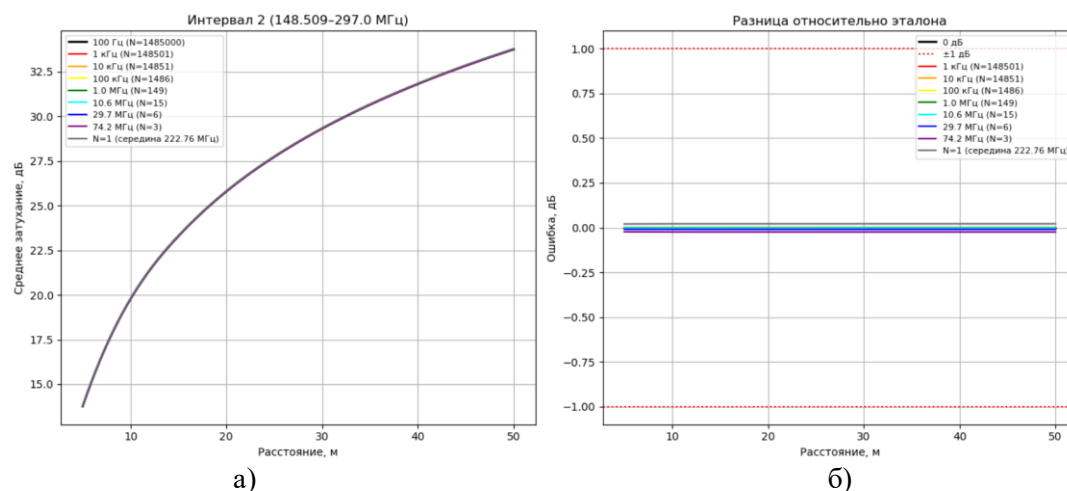


Рисунок 2 – Графики, рассчитанные по классической методике для 2-го частотного интервала для различного шага изменения частоты в зависимости от расстояния до СВТ: среднего затухания ПЭМИ $\bar{V}_r(\Delta F_j)$ (а) и ошибок измерения затухания (б)

Таблица 1

Ошибки измерения затухания ПЭМИ $\bar{\Delta V}_r(\Delta F_j, N_j)$, рассчитанные по классической методике в зависимости от количества точек расчета N

Номер интервала	Дальность, м	Ошибки измерения затухания ПЭМИ $\bar{\Delta V}_r(\Delta F_j, N_j)$, дБ, в зависимости от количества точек расчета N								
		1485000	148500	14850	1485	148	15	6	3	1
1	5	0	0	0,01	0,05	0,50	4,28	7,91	10,90	-12,80
	10	0	0	0,01	0,06	0,60	5,00	8,76	11,70	-12,50
	15	0	0	0,01	0,06	0,60	4,90	8,61	11,60	-12,20
	25	0	0	0,01	0,06	0,58	4,85	8,52	11,50	-12,01
	50	0	0	0,01	0,01	0,57	4,81	8,47	11,45	-12,00
2	5	0	0	0	0	0	0	-0,01	-0,02	0,02
	10	0	0	0	0	0	0	-0,01	-0,02	0,02
	15	0	0	0	0	0	0	-0,01	-0,02	0,02
	25	0	0	0	0	0	0	-0,01	-0,02	0,02
	50	0	0	0	0	0	0	-0,01	-0,02	0,02

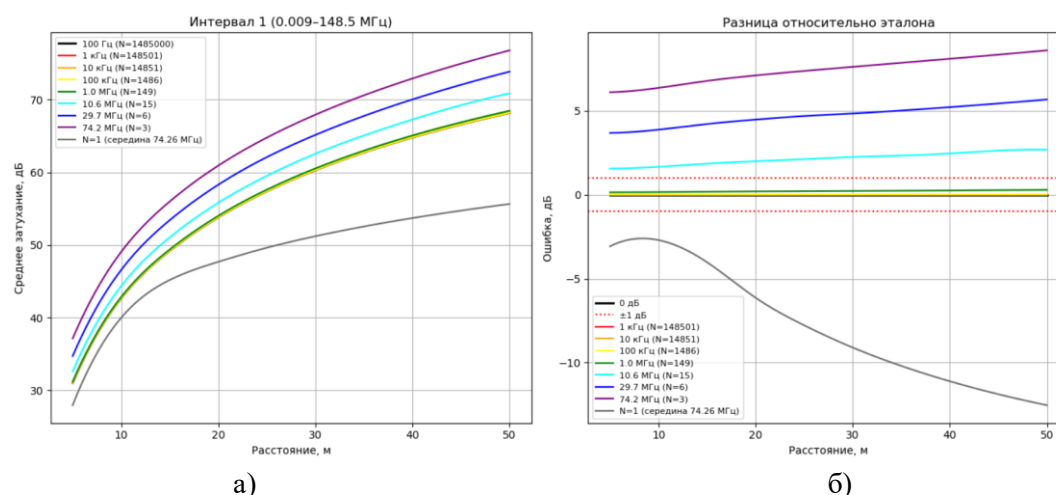


Рисунок 3 – Графики, рассчитанные по упрощенной методике ($R_{03} = 3\lambda$) для 1-го частотного интервала для различного шага изменения частоты в зависимости от расстояния до СВТ: среднего затухания ПЭМИ $\bar{V}_r(\Delta F_j)$ (а) и ошибок измерения затухания (б)

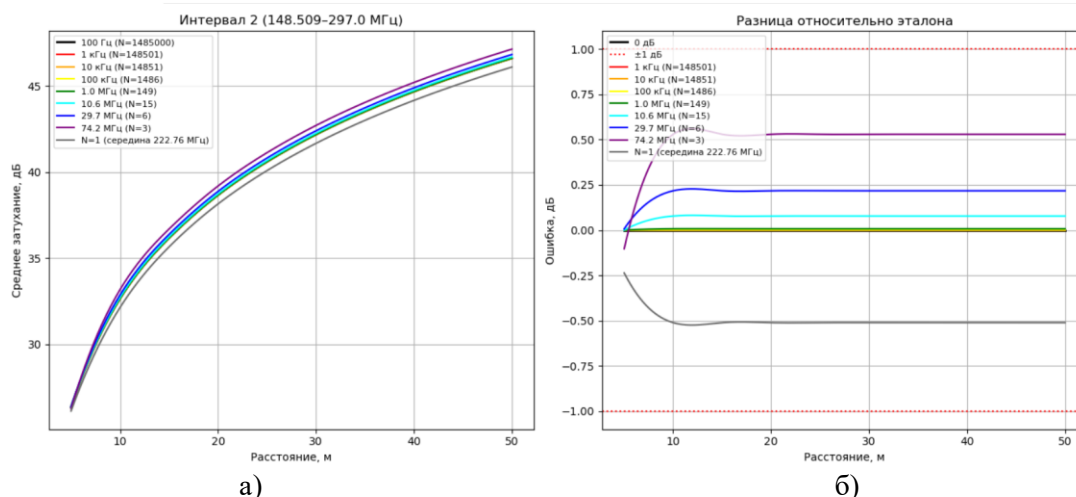


Рисунок 4 – Графики, рассчитанные по упрощенной методике ($R_{03} = 3\lambda$) для 2-го частотного интервала для различного шага изменения частоты в зависимости от расстояния до СВТ: среднего затухания ПЭМИ $\bar{V}_r(\Delta F_j)$ (а) и ошибок измерения затухания (б)

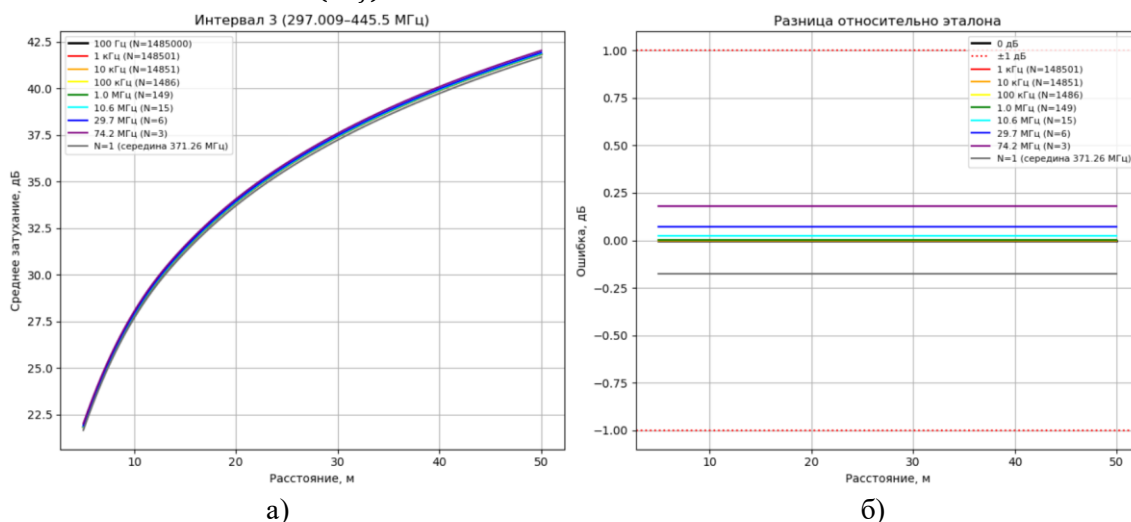


Рисунок 5 – Графики, рассчитанные по упрощенной методике ($R_{03} = 3\lambda$) для 3-го частотного интервала для различного шага изменения частоты в зависимости от расстояния до СВТ: среднего затухания ПЭМИ $\bar{V}_r(\Delta F_j)$ (а) и ошибок измерения затухания (б)

Таблица 2

Ошибки измерения затухания ПЭМИ $\bar{\Delta V}_r(\Delta F_j, N_j)$, рассчитанные по упрощенной методике ($R_{03} = 3\lambda$) в зависимости от количества точек расчета N

Номер интервала	Дальность, м	Ошибки измерения затухания ПЭМИ $\bar{\Delta V}_r(\Delta F_j, N_j)$, дБ, в зависимости от количества точек расчета N								
		1485000	148500	14850	1485	148	15	6	3	1
1	5	0	0	0	0,01	0,14	1,56	3,68	6,10	-3,07
	10	0	0	0	0,01	0,15	1,66	3,87	6,30	-2,70
	15	0	0	0	0,01	0,17	1,85	4,21	6,70	-4,02
	25	0	0	0	0,02	0,21	2,11	4,68	7,40	-7,70
	50	0	0	0	0,03	0,29	2,68	5,67	8,59	-12,54
2	5	0	0	0	0	0,01	0,01	0,01	-0,10	-0,23
	10	0	0	0	0	0,01	0,01	0,20	0,53	-0,51
	15	0	0	0	0	0,01	0,01	0,20	0,53	-0,51
	25	0	0	0	0	0,01	0,01	0,20	0,53	-0,51
	50	0	0	0	0	0,01	0,01	0,20	0,53	-0,51
3	5	0	0	0	0	0	0,03	0,07	0,18	-0,17
	10	0	0	0	0	0	0,03	0,07	0,18	-0,17
	15	0	0	0	0	0	0,03	0,07	0,18	-0,17

4	25	0	0	0	0	0	0,03	0,07	0,18	-0,17
	50	0	0	0	0	0	0,03	0,07	0,18	-0,17
	5	0	0	0	0	0	0,01	0,04	0,09	-0,09
	10	0	0	0	0	0	0,01	0,04	0,09	-0,09
	15	0	0	0	0	0	0,01	0,04	0,09	-0,09
	25	0	0	0	0	0	0,01	0,04	0,09	-0,09
	50	0	0	0	0	0	0,01	0,04	0,09	-0,09

Вывод: учитывая, что в соответствии с требованиями ФСТЭК России ошибка измерения амплитуды сигналов для не должна превышать ± 2 дБ, для оценочных расчетов затухания ПЭМИ можно использовать шаг изменения частоты: для 1-го частотного – не более 1 МГц ($N = 148$), а начиная со 2-го частотного интервала – достаточно рассчитать затухание на центральной частоте каждого частотного интервала.

Литература

1. Хорев А.А. Некоторые подходы к оценке возможностей перехвата побочных электромагнитных излучений средств вычислительной техники, использующих цифровые интерфейсы// Вестник УрФО «Безопасность в информационной сфере». – Челябинск, УрФО. – 2022. - № 3(45) – С. 5 – 16 ISSN: 2225-5435
2. Хорев А.А., Борисов Р.М. Методика расчета затухания побочных электромагнитных излучений средств вычислительной техники// Всероссийская конференция «Радиоэлектронные устройства и системы для инфотелекоммуникационных технологий – РЭУС-2026». Доклады. – М.: РНТОРЭС имени А.С. Попова. 2026. – С. ISBN 978-5-905278-62-4

JUSTIFICATION OF A RATIONAL STEP OF FREQUENCY CHANGES IN THE CALCULATION OF THE ATTENUATION OF PARTIAL ELECTROMAGNETIC RADIATION OF COMPUTER EQUIPMENT

prof. Horev A.A., stud. Borisov R.M.

National Research University of Electronic Technology

The article provides a justification for the rational frequency change step in the calculation of the attenuation of side electromagnetic emissions from computer equipment, based on the classical method based on D. Maxwell's theory and the simplified method based on the assumption that in the near zone, the field strength decreases inversely proportional to the cube of the distance ($E \sim 1/r^3$), in the middle zone, it decreases inversely proportional to the square of the distance ($E \sim 1/r^2$), and in the far zone, it decreases inversely proportional to the distance ($E \sim 1/r$). The calculations show that the minimum frequency change step should be at least 25-50 MHz (6-3 points per frequency interval).



МЕТОДИКА ФОРМИРОВАНИЯ РЕЧЕПОДОБНОЙ ПОМЕХИ НА ОСНОВЕ ЗВУКОВ РУССКОЙ РЕЧИ

студ. Букинин П.А.

Национальный исследовательский университет «МИЭТ»

Рассматривается методика формирования речеподобной помехи на основе звуков русской речи. Методика включает последовательное усреднение повторных реализаций звука у каждого диктора, формирование для каждого звука трёх вариантов помехи – мужской, женской и смешанной, а также подготовку тестовых стимулов для предварительной оценки разборчивости. Предлагаемый подход ориентирован на поэтапный отбор наиболее эффективных вариантов помех по результатам прослушивания и может быть использован как основа для последующих артикуляционных испытаний при исследовании защиты речевой информации.

Введение

Для защиты акустической речевой информации от утечки по техническим каналам широко применяются системы активной защиты, использующие шумовые и речеподобные помехи. Последние представляют особый интерес: их спектрально-временные характеристики близки к характеристикам маскируемого речевого сигнала, что потенциально обеспечивает более высокую маскирующую эффективность по сравнению с широкополосным шумом [1].

Вместе с тем сравнительная эффективность речеподобных помех, сформированных из речи дикторов разного пола, изучена недостаточно. В связи с этим требуется разработка и программная реализация методики, позволяющей систематически формировать необходимые виды речеподобных помех и в дальнейшем оценивать их маскирующие свойства в ходе артикуляционных испытаний.

Целью настоящей работы является представление методики формирования речеподобной помехи на основе звуков русской речи (далее – речеподобной помехи), ориентированную на поэтапное построение эталонных сигналов, получение мужских, женских и смешанных вариантов помехи для каждого звука.

Исходные данные

Исходными данными являются записи отдельных звуков русской речи, произнесенных группой дикторов. Первым шагом методики является выделение повторных реализаций звуков из непрерывной записи – для каждого диктора и каждого исследуемого звука. Пример такой фонограммы представлен на рисунке 1. Далее выполняется выравнивание выделенных реализаций по времени и их усреднение.

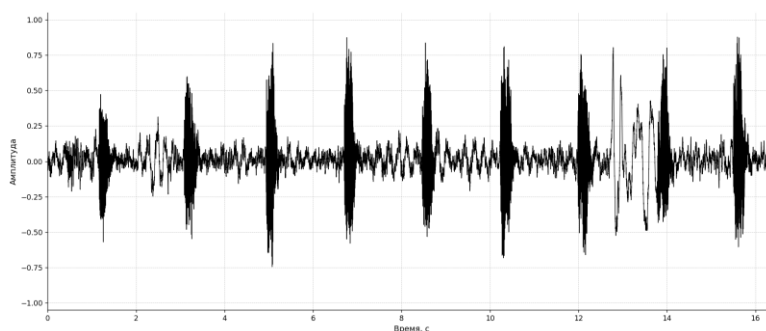


Рисунок 1 – Фонограмма звуков «а», произносимых одним диктором

Вторым шагом является уравнивание и усреднение представленных повторных реализаций звука, в результате которых для каждого сочетания «диктор — звук» формируется один эталонный сигнал, характеризующий данный звук у конкретного диктора. Усреднение происходит как для мужских дикторов, так и для женских. На рисунке 2 приведена фонограмма эталонного сигнала для звука «а», полученного усреднением его повторных реализаций, представленных на рисунке 1.

Такой подход позволяет уменьшить влияние случайных различий между отдельными произнесениями одного и того же звука одним диктором и получить более устойчивый сигнал, пригодный для последующего междикторного усреднения [2].

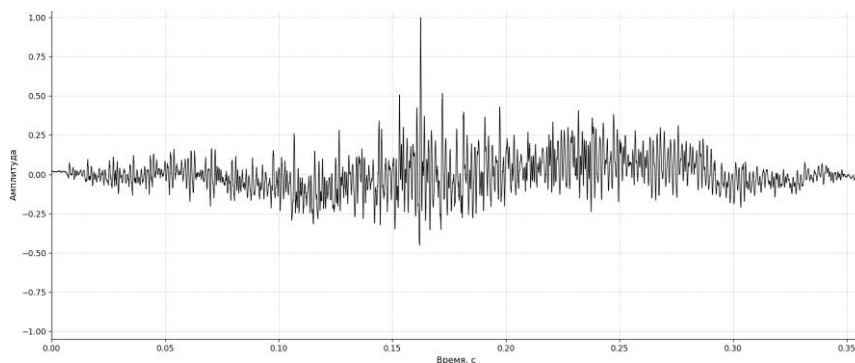


Рисунок 2 – Фонограмма звука «а», усредненная для одного дикторов

Третий шаг методики, а именно процесс формирования речеподобной помехи, основан уже не отдельных звуках одного диктора, а на звуках, усредненных для всех дикторов. Такой подход позволяет перейти к получению помехового сигнала, в меньшей степени зависящего от индивидуальных особенностей произношения одного диктора. Структура программной реализации указанных этапов представлен на рисунке 3.



Рисунок 3 - Структура программного комплекса подготовки речеподобных помех и стимулов

Программная реализация модуля сегментации и усреднения (M1) предназначена для выделения отдельных реализаций звука в непрерывной записи одного диктора и формирования усредненного эталонного сигнала. Обработка начинается с выбора временного окна, внутри которого содержатся повторы одного и того же звука [3]. Затем по кадрам (длительность FRAME_MS = 10 мс, шаг HOP_MS = 5 мс) рассчитывается среднеквадратичное значение, по локальному порогу определяются интервалы речевой активности.

После выделения интервалов выполняется их фильтрация по длительности: сегменты короче MIN_SEG_MS = 70 мс или длиннее MAX_SEG_MS = 1000 мс сразу исключаются. По оставшимся сегментам добавляется временной запас PAD_MS = 8 мс, отбираются наиболее информативные реализации (не более заданного количества произносимых повторов звука), выполняется их выравнивание по максимуму амплитуды и финальное усреднение. Алгоритм наиболее наглядно показан на рисунке 4.

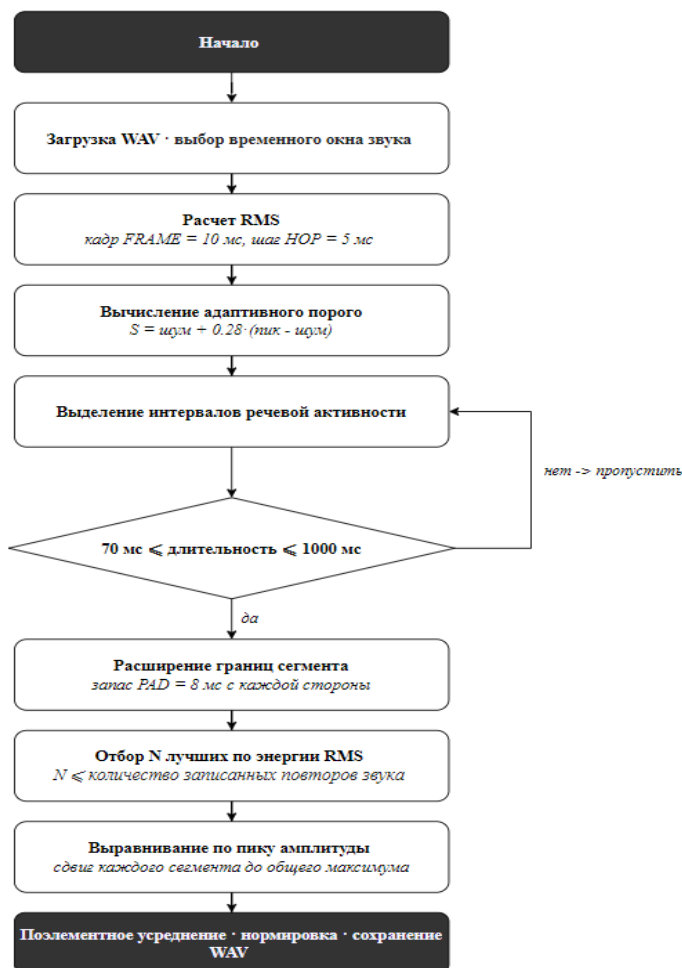


Рисунок 4 – Алгоритм модуля сегментации и усреднения реализаций звука

Модуль формирования междикторной речеподобной помехи (M2) реализует построение речеподобной помехи для заданного звука на основе нескольких дикторов [4]. Помеха формируется в трех вариантах: мужском, женском и смешанном, представляющем собой усредненную смесь сигналов мужских и женских дикторов. Фонограмма сформированной мужской междикторной помехи для звука «а» представлена на рисунке 5.

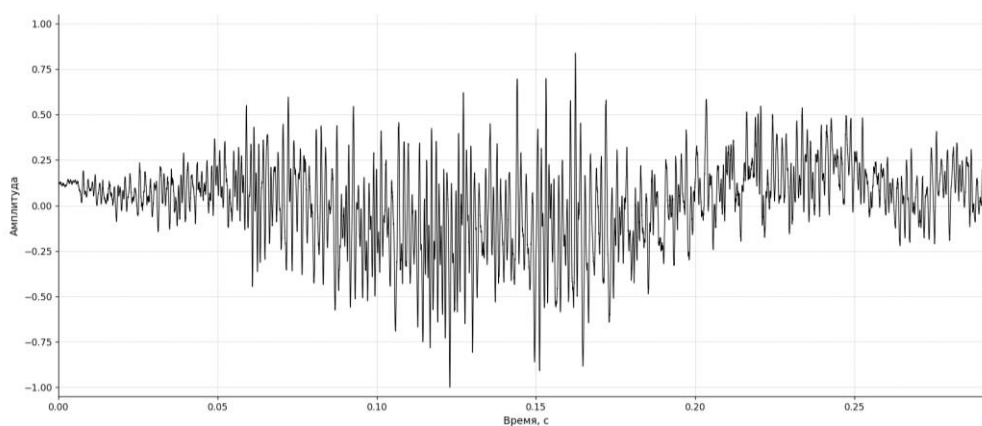


Рисунок 5 – Фонограмма звука «а», усредненная по всем дикторам-мужчинам и представляющая собой готовую речеподобную помеху

Таким образом, модуль сегментации и усреднения обеспечивает автоматизированное выделение информативных реализаций звука из непрерывной записи диктора и формирование усреднённого эталонного сигнала, а второй модуль, в свою очередь, позволяет сформировать междикторную речеподобную помеху, которая в дальнейшем используется для оценки её маскирующей эффективности.

Формирование зашумленных стимулов

Четвертым шагом является создание зашумленного стимула путем наложения на скрываемый сигнал подготовленной речеподобной помехи с учетом параметров отношения сигнал/шум q и временного смещения τ [5]. В качестве скрываемого сигнала используется один мужской и один женский диктор, имеющие достаточно четкое произношение. Структура программного комплекса для формирования зашумленных смесей представлена на рисунке 6.

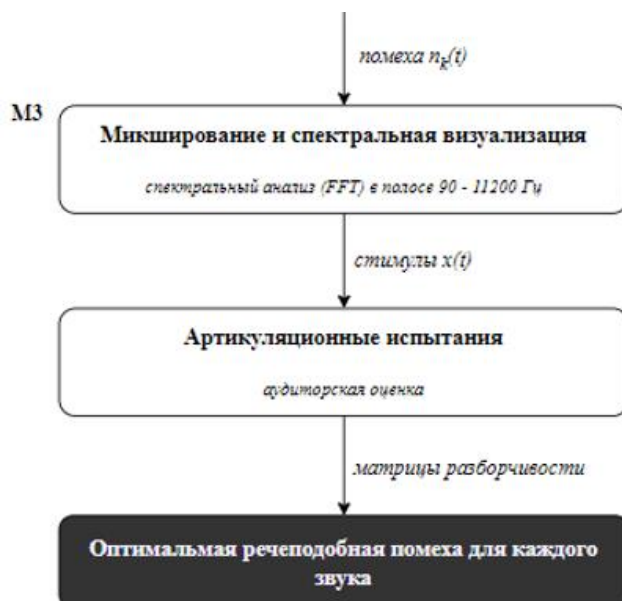


Рисунок 6 – Структура программного комплекса для формирования зашумленных смесей

Фонограмма смеси сигнал + шум, где в качестве скрываемого сигнала используется звук «а», а в качестве шума – речеподобная помеха, сформированная на основе звука «и», представлена на рисунке 7.

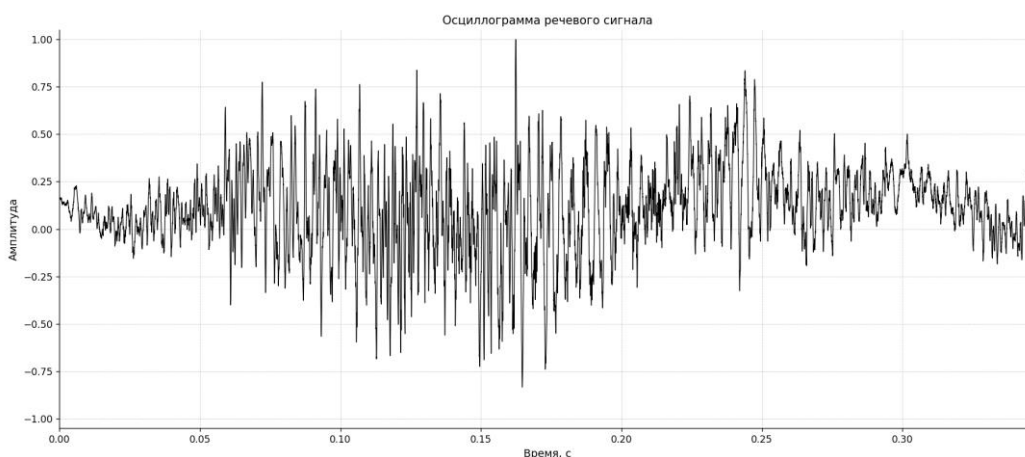


Рисунок 7 – Фонограмма смеси сигнал + шум, где в качестве скрываемого сигнала используется звук «а», а в качестве шума – речеподобная помеха, сформированная на основе звука «и»

Таким образом, подготовленная смесь маскируемого сигнала и речеподобной помехи используется в артикуляционных испытаниях для выбора наиболее оптимальной помехи.

Оценка эффективности речеподобных помех проводится в следующем порядке:

1. Выбираются два диктора (мужского и женского пола) с наиболее чёткой артикуляцией используемых звуков.
2. На исходные звуки последовательно накладываются три варианта помех: мужская, женская и смешанная.
3. По критерию воспринимаемого качества зашумленных звуков определяется оптимальный тип помехи.

Результаты испытаний представляют в виде таблицы, где помехи ранжированы по убыванию степени их маскирующего воздействия - от максимально эффективной до практически не влияющей на разборчивость сигнала.

Разработанная методика обеспечивает системный подход к формированию речеподобных помех, формируемых из звуков русской речи. Методика включает последовательные этапы - усреднение и

выравнивание звуков у одного диктора, формирование междикторной помехи, а также создание смеси «скрываемый звук-речеподобная помеха». Ее реализация позволит определить оптимальные речеподобные помехи для каждого звука русской речи и построить аналитические зависимости, образующие научную базу для проектирования и оценки эффективности систем виброакустической защиты речевой информации.

Литература

1. Хорев А.А., Дворянкин С.В., Козлачков С.Б., Василевская Н.В. Анализ предельных возможностей методов шумопонижения и реконструкции речевых сигналов, маскируемых различными типами помех // Вопросы кибербезопасности. — 2024. — № 1 (59).
2. Дворянкин С.В., Дворянкин Н.В., Устинов Р.А. Речеподобные помехи, устойчивые к методам шумоподавления в результате скремблирования защищенной речи // Вопросы кибербезопасности. — 2022. — № 5(51). — С. 14-27.
3. Авдеев В.Б., Трушин В.А., Кунгуров М.А. Унифицированные речеподобные помехи для активной защиты речевой информации // Informatics and Automation. — 2020. — Т. 19. — № 5. — С. 991-1017.
4. Волчихина М.В. Алгоритм формирования адаптивной речеподобной помехи для защиты конфиденциальной речевой информации в офисных помещениях // Proceedings of Telecommunication Universities. — 2025. — Т. 11. — № 5. — С. 21-27.
5. Васильев Р.А. Метод создания защищенной речеподобной помехи с идентификацией голоса [Электронный ресурс]. — URL: <https://cyberleninka.ru/article/n/metod-sozdaniya-zaschischyonnoy-rechepodobnoy-pomehi-s-identifikatsiey-golosa/viewer> (дата обращения: 29.01.2026).

THE METHOD OF FORMING SPEECH-LIKE INTERFERENCE BASED ON THE SOUNDS OF RUSSIAN SPEECH

stud. Bukinin P.A.

National Research University of Electronic Technology

The method of forming speech-like interference based on the sounds of Russian speech is considered. The technique includes sequential averaging of repeated sound implementations for each speaker, the formation of three interference variants for each sound – male, female and mixed, as well as the preparation of test stimuli for a preliminary assessment of intelligibility. The proposed approach focuses on the step-by-step selection of the most effective interference options based on listening results and can be used as a basis for subsequent articulation tests in the study of speech information protection.



МОДЕЛИРОВАНИЕ ФУНКЦИОНИРОВАНИЯ БЕСПРОВОДНОЙ СЕТИ Wi-Fi ПРОМЫШЛЕННОЙ АСУ ТП В УСЛОВИЯХ ВОЗДЕЙСТВИЯ КИБЕРУГРОЗ

асп. Буренок Д.С.

Национальный исследовательский университет «МИЭТ»

В работе рассмотрены вопросы моделирования функционирования беспроводной сети Wi-Fi промышленной АСУ ТП в условиях воздействия киберугроз. Выделены ключевые элементы модели, мотивирован метод моделирования, а также обозначены ожидаемые результаты. Выбранный подход к моделированию учитывает структуру АСУ ТП, специфику функционирования беспроводных сетей Wi-Fi, возможности и ограничения средств мониторинга, а также актуальные угрозы информационной безопасности. Представлены промежуточные результаты моделирования, включая моделирование зависимости обнаружения точек доступа Wi-Fi для заданных пороговых значений от времени, оценку вероятности и времени обнаружения атаки при заданных параметрах мониторинга. Осуществлено сопоставление отдельных результатов с ранее полученными экспериментальными данными, что подтвердило корректность выбранного подхода к моделированию.

Ввиду требований к обеспечению информационной безопасности промышленных АСУ ТП [1, 2] проведение инструментального тестирования защищенности сетевой инфраструктуры (пентест) представляет из себя дополнительный фактор риска. Так, нарушение сетевой связности компонентов АСУ ТП, например, в результате тестовой атаки на Wi-Fi сеть, может привести к останову технологического процесса. Моделирование является безопасной альтернативой.

В контексте моделирования функционирования беспроводной сети Wi-Fi промышленной АСУ ТП в условиях воздействия киберугроз важно учесть следующие ключевые аспекты:

- структура АСУ ТП;
- специфика функционирования беспроводных сетей Wi-Fi;
- возможности и ограничения средств мониторинга;
- актуальные угрозы информационной безопасности.

Так как моделирование осуществляется в отношении беспроводной сети Wi-Fi АСУ ТП, сетевая топология соответствующей системы должна быть учтена в модели. Предлагается использовать представление соответствующей сети в виде графа, вершины которого характеризуют ключевые узлы АСУ ТП, а ребра – каналы связи, в т.ч. беспроводные сети Wi-Fi. Аналогичный подход использовался автором ранее в [3, 4].

Применительно к функционированию канала связи Wi-Fi важны ограничения и специфика протоколов передачи данных семейства IEEE 802.11 [5], включая канальное деление, потеря пакетов, структура фреймов данных. Также должен быть учтен транспортный уровень TCP/UDP.

В отношении программно-аппаратных средств мониторинга беспроводной сети Wi-Fi важны следующие аспекты, выделенные в работе [6]:

- расширение радиочастотного диапазона в последнем поколении стандартов IEEE 802.11 требует осуществления мониторинга в широком диапазоне радиочастот;
- средства мониторинга должны быть сконфигурированы и размещены таким образом, чтобы обеспечить прием пакетов с заданным значением доли пропуска;
- средства мониторинга должны иметь возможность оперативно раскрывать присутствующие в радиоэфире приемо-передающие устройства, включая точки доступа Wi-Fi и их абонентов;
- средства мониторинга должны обеспечивать возможность определения местоположения устройства, с использованием которого осуществляется атака на Wi-Fi сеть.

Актуальные угрозы информационной безопасности [7], состав и содержание мер обеспечения информационной безопасности [1], известные уязвимости отражают возможную поверхность атаки и также должны иметь отражение в модели.

Таким образом, при составлении модели вышеперечисленные аспекты должны быть учтены посредством математической формализации и взаимоувязаны логически. Перспективно использовать имитационное моделирование и сопоставление результатов с эмпирическими данными, полученными в результате экспериментальных исследований.

В качестве источника экспериментальных данных может выступать работа автора [8]. Были проведены экспериментальные исследования, устанавливающие взаимосвязь между порядком осуществления мониторинга и обнаружением поддельных и несанкционированных точек доступа Wi-Fi. Исследовались следующие параметры:

- интервал сканирования радиоканала (0,05; 0,15; 0,4; 0,8; 1,6; 3,2; 6,5 секунд);
- последовательность переключения радиоканалов (последовательное, случайное).

Был построен график зависимости обнаружения точек доступа для заданных пороговых значений от времени – рисунок 1. На рисунке 2 представлена разница во времени достижения пороговых значений в зависимости от последовательности переключения каналов. Сканирование при последовательном переключении радиоканалов, по сравнению со случайным переключением радиоканалов, выигрывает в скорости достижения пороговых значений. Независимо от последовательности переключения радиоканалов, сравнительно небольшой интервал сканирования одного радиоканала позволяет проводить более оперативное обнаружение точек доступа.

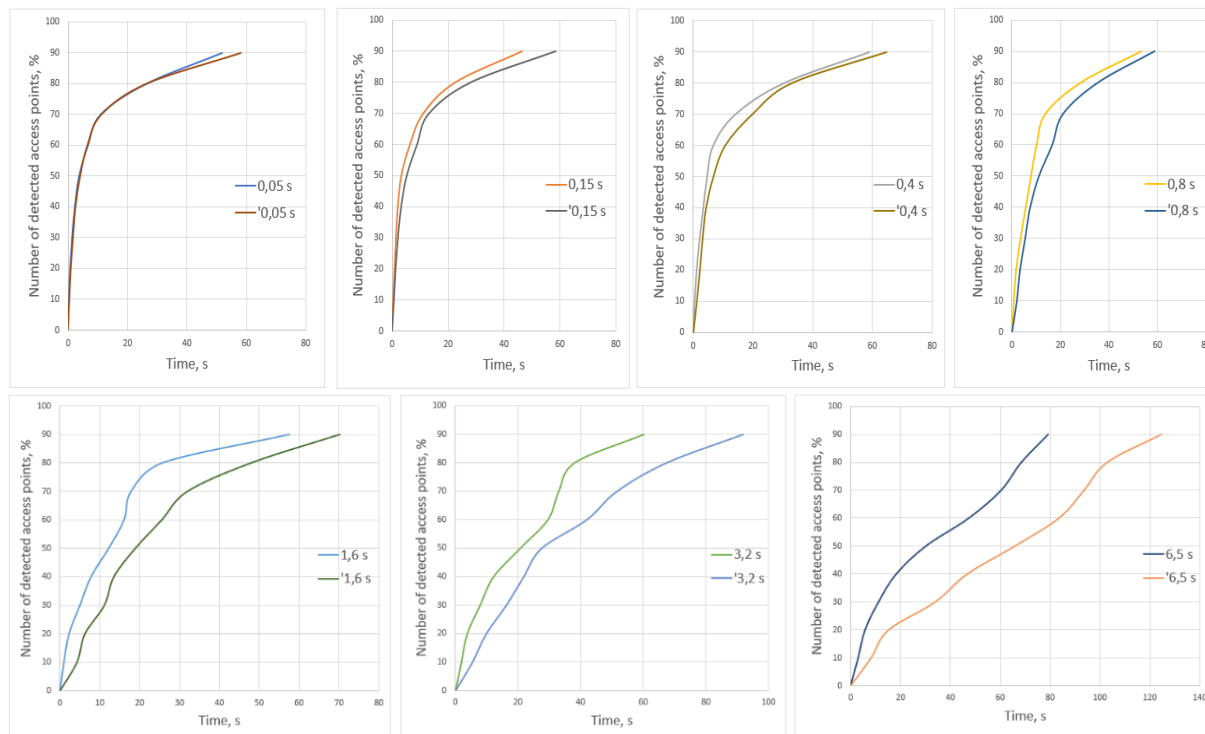


Рисунок 1 – Зависимость обнаружения точек доступа для заданных пороговых значений от времени

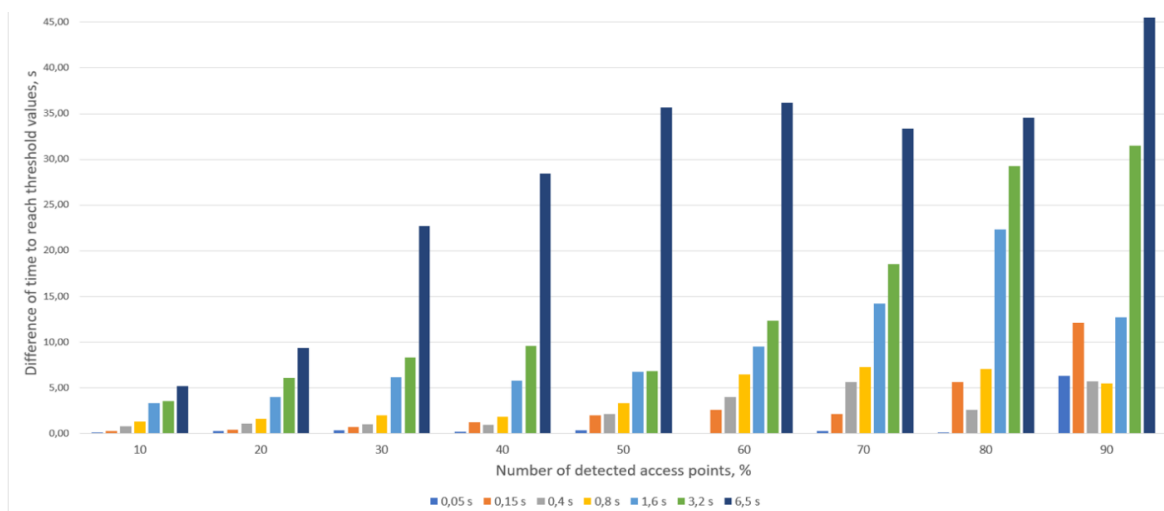


Рисунок 2 – Разница во времени достижения пороговых значений при последовательном и случайном переключении радиоканалов

При работе средства мониторинга на оптимальных параметрах достигается увеличение скорости обнаружения атак (например, распространен способ обнаружения DDoS-атак на Wi-Fi сеть [9], скорость работы которого зависит от времени построения репрезентативной выборки пакетов деаутентификации и диссоциации), что должно иметь отражение в модели.

Модель должна основываться на передаче данных по Wi-Fi посредством приема и отправки пакетов. В т.ч. предоставлять возможность теоретического расчета количества пакетов конкретного типа, которые могут быть приняты средствами мониторинга при определенных параметрах, позволять оценить вклад соответствующих параметров в эффективность мониторинга. Для формализации процесса приема Wi-Fi пакетов в рамках мониторинга предлагается использовать формулу (1):

$$Pkts_{захваченные}^{тип X}(\tau) = a \cdot \sum_{j=1}^n \left(\int_{t_0}^{t_0+\tau} \lambda_{c_j}(t) \cdot w_{c_j}(t) \cdot (1 - P_{c_j}^{err}(t)) \cdot r_j^{тип X}(t) \cdot dt \right), \quad (1)$$

- где
- n — количество радиоканалов;
 - a — коэффициент масштабирования;
 - $\lambda_{c_j}(t)$ — мгновенная интенсивность случайной величины отправленных пакетов в пределах радиоканала;
 - $w_{c_j}(t)$ — оконная функция, определяющая порядок осуществления мониторинга;
 - $P_{c_j}^{err}(t)$ — вероятность ошибки на пакет;
 - $r_j^{тип X}(t)$ — доля пакетов определенного типа.

Имитационное моделирование позволяет воспроизвести процесс в случаях, когда подинтегральные функции не могут быть заданы аналитически. Результаты имитационного моделирования раскрытия сведения о Wi-Fi сети АСУ ТП промышленного объекта представлены на рисунке 3. Полученные в результате моделирования данные по форме зависимости сопоставимы с экспериментальными данными, представленными в [8].

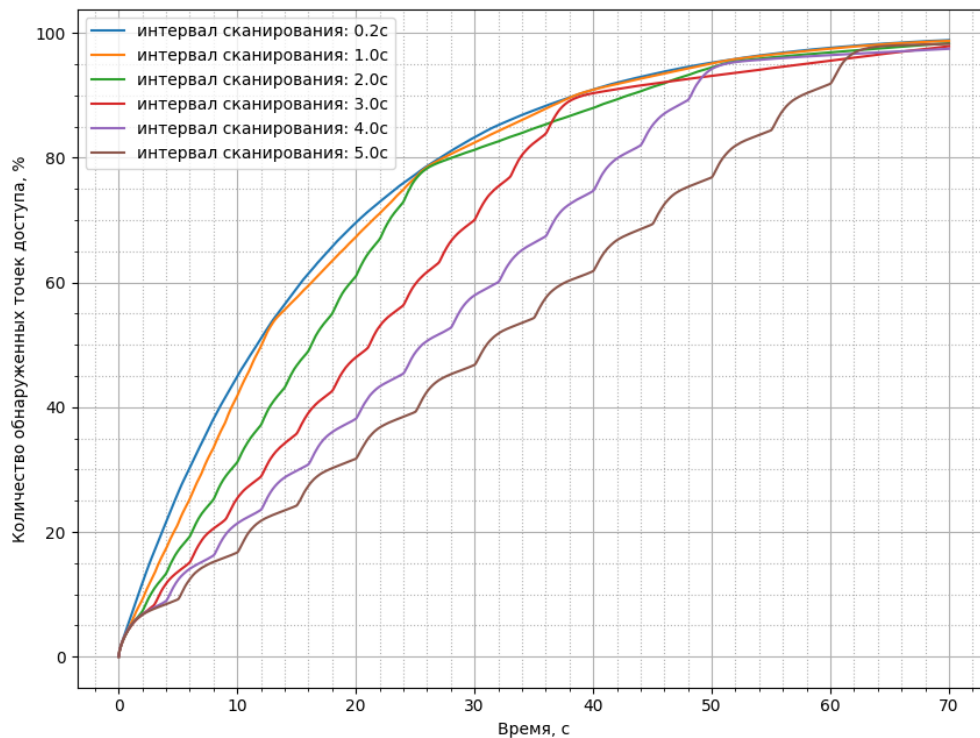


Рисунок 3 – Результат имитационного моделирования зависимости обнаружения точек доступа Wi-Fi для заданных пороговых значений от времени

На основе формулы (1) возможно оценить вероятность $P_{детект}$ и время t обнаружения атаки для алгоритма с вероятностью детектирования $P_{алгоритма}$ и интервалом отправки злоумышленником пакетов $\omega_{отпр}$ при вероятности приема средством мониторинга $P_{приема}$. Варианты графиков, которые могут быть построены с использованием аппарата теории вероятности [10], представлены на рисунках 4 и 5.

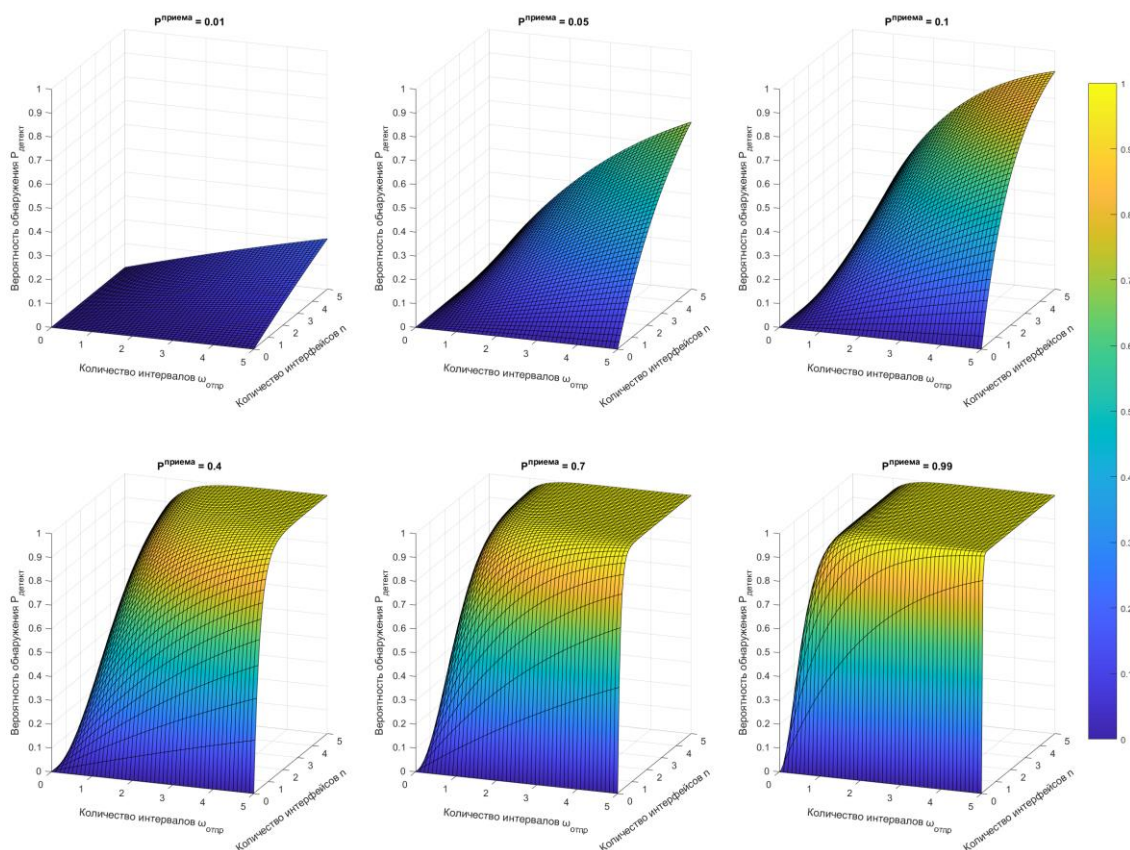


Рисунок 4 – Оценка вероятности обнаружения атаки при заданных параметрах мониторинга

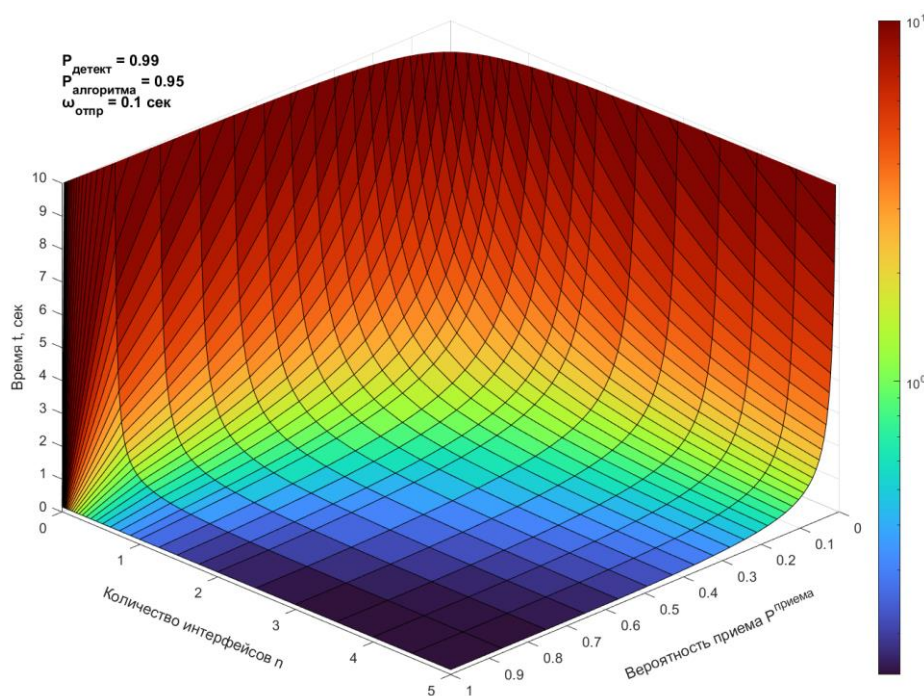


Рисунок 5 – Оценка времени обнаружения атаки при заданных параметрах мониторинга

В результате работы определены подходы к моделированию, в том числе выделены ключевые элементы модели, мотивирован метод моделирования, а также обозначены ожидаемые результаты. После проведения апробации на конференции планируется внести корректировки в модель на основе полученной обратной связи, формализовать модель, разработать программное обеспечение для моделирования и провести экспериментальные исследования с разработанной моделью. Полученные результаты будут использованы в основе кандидатской диссертации на соискание ученой степени кандидата технических наук в качестве

выносимой на защиту модели функционирования беспроводной сети Wi-Fi промышленной АСУ ТП в условиях воздействия киберугроз.

Литература:

1. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Справочная правовая система КонсультантПлюс [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 24.03.2026).
3. Буренок Д. С., Воеводин В. А. Моделирующее устройство для оценки весомости узлов в сетях управления критической информационной инфраструктуры // Роспатент. Патент на полезную модель № 228273 от 21.08.2024.
4. Буренок Д. С., Воеводин В. А. Моделирующее устройство для оценки доступности информации в сетях управления критической информационной инфраструктуры // Роспатент. Патент на полезную модель № 217283 от 24.03.2023.
5. Geraci G., Meneghello F., Wilhelmi F., Lopez-Perez D., Val I., Galati G. L., Cordeiro C., Ghosh M., Knightly E., Bellalta B. Wi-Fi: Twenty-five years and counting. *Proceedings of the IEEE*, pp. 1-47. doi:10.1109/JPROC.2026.3662513
6. Буренок Д.С. Проблематика мониторинга информационной безопасности беспроводных сетей Wi-Fi в АСУ ТП промышленного типа // 32-я Всероссийская межвузовская научно-техническая конференция студентов и аспирантов с международным участием “Микроэлектроника и информатика -2025”, 24 – 25 апреля 2025 года, г. Зеленоград.
7. Банк данных угроз безопасности информации // ФСТЭК России [Электронный ресурс]. – URL: <https://bdu.fstec.ru/threat> (дата обращения: 24.03.2026).
8. Burenok D. S. Experimental Study of Sequential and Random Channel Hopping for Detecting Wi-Fi Access Points // 2022 International Siberian Conference on Control and Communications (SIBCON), Tomsk, Russian Federation, 2022. doi: 10.1109/SIBCON56144.2022.10003009.
9. Agarwal M., Biswas S., Nandi S. Detection of De-authentication Denial of Service attack in 802.11 networks. 2013 Annual IEEE India Conference (INDICON). Mumbai, 2013, pp. 1-6. doi: 10.1109/INDICON.2013.6726015
10. Dekking F.M., Kraaikamp C., Lopuhaa H.P., Meester L.E. A Modern Introduction to Probability and Statistics, Understanding Why and How. Springer Texts in Statistics, Springer, 2005, 486 p. – ISBN 978-1-85233-896-1, doi: 10.1007/1-84628-168-7.

APPROACH TO MODELING Wi-Fi NETWORK OPERATION FOR AN INDUSTRIAL CONTROL SYSTEM UNDER THE IMPACT OF CYBER THREATS

Postgraduate Student Burenok D.S.

National Research University of Electronic Technology

The paper outlines modeling of an industrial Wi-Fi network under cyberthreat conditions. Key elements of the model are highlighted, the modeling method is justified, and the expected results are outlined. The chosen modeling approach takes into account structure of the industrial Wi-Fi network, specifics of Wi-Fi network operation, capabilities and limitations of monitoring tools, and current information security threats. Intermediate modeling results are presented, including modeling the dependence of Wi-Fi access point detection for given threshold values on time, and an estimate of the probability and time of attack detection under given monitoring parameters. A comparison of partial results with previously obtained experimental data is performed, confirming the validity of the chosen modeling approach



РАЗРАБОТКА ЗАЩИЩЁННОЙ СИСТЕМЫ ПЕРЕДАЧИ И ХРАНЕНИЯ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ И ПОРОГОВЫХ СХЕМ

студ. Баранова Е.И.¹, доц. Бутакова Н.Г.^{1,2},
студ. Винник Е.А.¹, студ. Филиппова П.В.¹

¹Московский политехнический университет

²Национальный исследовательский университет «МИЭТ»

В работе рассматривается архитектура защищённой системы передачи и хранения криптографических ключей, включающая алгоритмы постквантового обмена ключами, аутентификации на основе доказательства с нулевым разглашением и распределённого хранения ключевого материала с использованием пороговых схем. Анализируются преимущества защиты такой архитектуры в условиях роста киберугроз, криптографической устойчивости и отказоустойчивости системы к квантовым атакам. Обсуждаются перспективы применения предлагаемой архитектуры для защиты информационного обмена на распределённых объектах от квантовых угроз.

Развитие распределённых информационных систем сопровождается ростом требований к защите данных, криптографических ключей и механизмов аутентификации. Одновременно усиливаются угрозы, связанные с перехватом трафика, компрометацией серверов и уязвимостями протоколов доступа. Дополнительный риск создаёт развитие квантовых вычислений, способных нарушить стойкость современных криптосистем, особенно построенных на проблемах факторизации большого числа и дискретного логарифмирования, включая эллиптически кривые [1].

Возникновение квантовой угрозы делает уязвимыми и криптографическую защиту данных, и процедуры аутентификации в процессах доступа, и сам обмен и хранение ключевого материала, настраивающего криптографические средства обеспечения целостности, конфиденциальности и аутентификации. Перспективным решением этой проблемы является объединение алгоритмов постквантового обмена ключами, порогового распределения секрета и протоколов доказательства знания без передачи самого секрета.

Для сопоставления классической и квантовой моделей используются оценки вычислительной сложности. В классической модели сложность факторизации больших целых чисел, лежащая в основе стойкости RSA-подобных схем, может быть оценена с использованием L-нотации следующим образом:

$$L\left[n^{\frac{1}{3}(\frac{64}{9})^{\frac{1}{3}}}\right] = \exp\left(\left(\left(\frac{64}{9}\right)^{\frac{1}{3}} + o(1)\right)(\ln n)^{\frac{1}{3}}(\ln \ln n)^{\frac{2}{3}}\right) \quad (1)$$

Формула (1) показывает, что при больших n задача факторизации остаётся крайне трудной для классических систем.

В квантовой модели сложность алгоритма Шора описывается следующим выражением:

$$T_{\{Shor\}} = O((\log n)^3) \quad (2)$$

Соотношение (2) отражает полиномиальный характер квантовой атаки и объясняет необходимость отказа от RSA-подобных механизмов, к которым относится и алгоритм обмена ключами Диффи-Хеллмана, широко используемый сегодня в сетевых технологиях.

Предлагаемая система обмена ключами приведена на рисунке 1 и представляет модульную архитектуру защиты генерации, распределения и хранения ключевого материала. На первом этапе выполняется аутентификация пользователя без передачи пароля, затем иницируется постквантовый обмен ключами, после чего сеансовый ключ или мастер-секрет разделяется на несколько долей и распределяется между независимыми узлами хранения. Распределённая архитектура снижает риск полной компрометации при взломе отдельного узла и позволяет адаптировать параметры алгоритмов под требуемый уровень безопасности и допустимые вычислительные затраты.

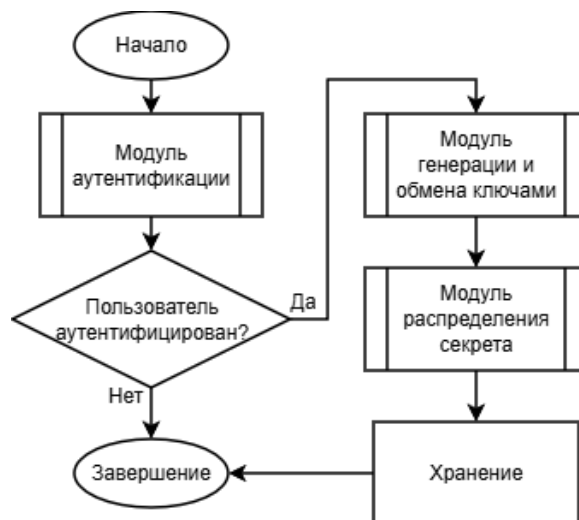


Рисунок 7 - Архитектура системы защищённой передачи и хранения ключей

Модуль аутентификации. Ключевым требованием к системе является отказ от хранения и передачи пароля в явном виде. Для аутентификации использовано доказательство знания с нулевым разглашением на основе протокола Шнорра [2]. Такой подход снижает риск утечки данных при перехвате трафика, однако требует защиты от атак с повтором и «человек посередине». На рисунке 2 представлена архитектура модуля аутентификации, в которую входят одноразовые идентификаторы сессии.

Пользователь, используя свой секретный ключ s , сформированный на этапе регистрации, формирует проверочное значение t , которое вычисляется путём возведения базового элемента группы g в степень случайного одноразового числа, выбранного для данной сессии, после чего отправляет значение t серверу. Сервер генерирует случайный вызов w в виде числового значения, после чего пользователь вычисляет отклик с использованием s и передаёт его обратно. Сервер проверяет отклик по открытым параметрам g , u , а также значениям t и w , и по результату проверки завершает аутентификацию.

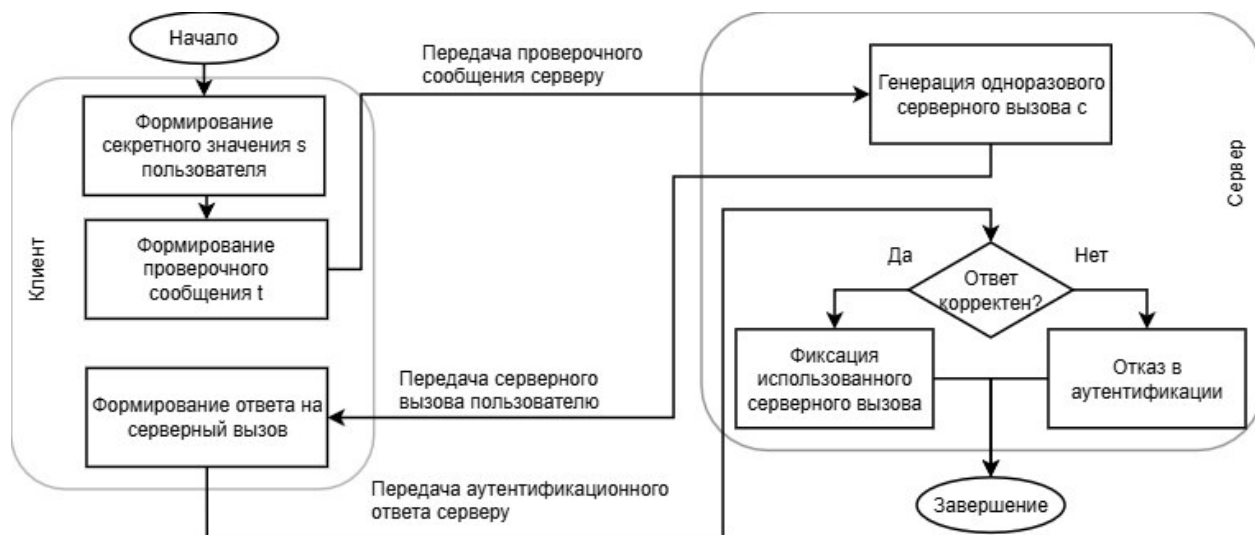


Рисунок 2 - Процедура доказательства знания секрета по протоколу Шнорра

Корректность доказательства знания секрета в протоколе Шнорра проверяется следующим условием:

$$g^s = t \cdot y^w \quad (3)$$

В равенстве (3) g обозначает базовый элемент группы, используемой в протоколе, t – начальное проверочное значение, сформированное пользователем, y – открытый ключ пользователя, вычисленный на основе его секретного ключа s , w – случайный одноразовый вызов сервера.

Вероятность успешной имитации аутентификации без знания секрета оценивается выражением:

$$P_{attack} = \frac{1}{q} \quad (4)$$

где q – число допустимых значений случайного вызова сервера.

При достаточно большом q выражение (4) даёт пренебрежимо малую вероятность ложной аутентификации.

Модуль генерации и обмена ключами. В качестве базового механизма обмена ключами предлагается использовать CRYSTALS-Kyber, основанный на задачах криптографии на решетках [3]. Алгоритм обеспечивает устойчивость к квантовым атакам и позволяет выбирать баланс между стойкостью и вычислительной нагрузкой за счёт нескольких уровней параметров.

В распределённой системе применение CRYSTALS-Kyber связано с увеличением размеров ключей и служебных сообщений, ростом трафика и необходимостью многократных операций инкапсуляции и декапсуляции. Для снижения этих издержек целесообразны кэширование сеансовых параметров и адаптивный выбор уровней Kyber512, Kyber768 или Kyber1024.

Стойкость CRYSTALS-Kyber связывается с задачей Learning With Errors (LWE – обучение с ошибками), которую в упрощённом виде можно представить равенством (5) [4]:

$$b = As + e \bmod q \quad (5)$$

В выражении (5) все элементы – полиномы, b – открытый ключ, A – публичная матрица, s – секретный ключ, e – маскирующий вектор (ошибка), q – модуль вычислений. Наличие ошибки делает восстановление секрета вычислительно сложным.

Отправителем генерируется случайный секретный ключ K . Ключ инкапсулируется – шифруется на открытом ключе получателя b и передается по открытому каналу получателю. Получатель расшифровывает секрет на своем секретном ключе s , то есть декапсулирует ключ K . Таким образом устанавливается общий секретный ключ.

Модуль распределения секрета. Для распределённой системы хранения важно сохранять высокую энтропию секретного материала. Это требование задаётся неравенством:

$$H(K) \geq 256 \quad (6)$$

В неравенстве (6) $H(K)$ – энтропия ключевого материала, K – ключевой материал или секретный ключ, подлежащий хранению и распределению. Данное неравенство означает, что уровень неопределённости секрета должен оставаться не ниже 256 бит.

Для отказоустойчивого хранения ключевой информации используется пороговая схема Шамира: секрет делится на n долей, а для его восстановления требуется не менее k долей, где $k \leq n$. Такой подход снижает риск полной компрометации данных при атаке на отдельный сервер.

Базовая схема Шамира не защищает от активных атак, связанных с подменой долей при восстановлении, поэтому в рассматриваемой архитектуре добавлена схема с проверкой секрета [5]. Схема представлена на рисунке 3. На первом этапе ключ K разделяется на доли и распределяется между узлами хранения, на основе ключа K формируется секрет, представляющий собой хэш-значение ключа. Секрет также независимо разделяется на доли и распределяется между узлами. Затем при восстановлении одновременно собираются доли ключа K и секрета, после чего по восстановленному секрету выполняется проверка корректности данных. При положительном результате проверки ключ K принимается как достоверный, а при отрицательном фиксируется нарушение целостности.



Рисунок 3 - Схема верификации ключа через секрет

Формально пороговое распределение секрета задаётся многочленом степени $k-1$:

$$f(x) = S + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1} \quad (7)$$

В формуле (7) S обозначает секрет, а коэффициенты $a_1, \dots, a_{k-1}$ выбираются случайно.

Восстановление секрета выполняется по интерполяционной формуле Лагранжа:

$$S = \sum_{i=1}^k f(x_i) \prod_{j=1, j \neq i}^k \frac{x_j}{x_j - x_i} \quad (8)$$

Соотношение (8) показывает, что для восстановления достаточно k корректных долей.

Вероятность компрометации системы при атаке на несколько узлов можно оценить биномиальной моделью:

$$P_{comp} = \sum_{i=k}^n C(n, i) p^i (1 - p)^{n-i} \quad (9)$$

В выражении (9) n – число узлов хранения, k – порог восстановления, p – вероятность компрометации одного узла.

Отказоустойчивость характеризуется вероятностью того, что система не сможет собрать достаточное количество долей:

$$P_{fail} = \sum_{i=0}^{k-1} C(n, i) (1 - r)^i r^{n-i} \quad (10)$$

В формуле (10) r обозначает вероятность отказа отдельного узла.

Для оценки риска повторного использования одноразовых параметров применяется приближение вероятности коллизии одноразового случайного значения:

$$P_{collision} = \frac{N^2}{2^{\{\lambda+1\}}} \quad (11)$$

В формуле (11) N обозначает количество сессий, а λ – длину одноразового случайного значения в битах.

Коммуникационные затраты постквантового обмена описываются через суммарный объём служебных данных:

$$V_{total} = PK + CT + overhead \quad (12)$$

В равенстве (12) PK обозначает открытый ключ получателя, который передаётся или используется в протоколе для инкапсуляции общего секрета, CT – шифртекст, то есть результат инкапсуляции, передаваемый по открытому каналу, а $overhead$ – дополнительные служебные поля протокола.

Время передачи этого объёма по каналу пропускной способности B определяется соотношением:

$$t = \frac{V_{total}}{B} \quad (13)$$

Формула (13) позволяет связать параметры постквантового обмена с сетевой задержкой.

Помимо криптографической стойкости базовых примитивов, система должна быть устойчива к практическим атакам. Необходимо учитывать компрометацию узлов хранения, подмену долей, атаки повторного воспроизведения и атаки посредника при аутентификации.

Отдельное внимание должно уделяться атакам по побочным каналам, прежде всего timing-атакам (атакам по времени). Поэтому реализация должна предусматривать алгоритмы с постоянным временем выполнения, маскирование промежуточных значений и аккуратную обработку исключений.

Если рассматривать основные уровни защиты как независимые рубежи, общую вероятность компрометации системы можно аппроксимировать произведением частных вероятностей:

$$P_{total} = p_1 \cdot p_2 \cdot p_3 \quad (14)$$

В выражении (14) p_1 , p_2 и p_3 интерпретируются как вероятности обхода аутентификации, компрометации порогового хранилища и нарушения защищённого обмена.

Интеграция постквантового обмена ключами, порогового распределения секрета и аутентификации на основе доказательства с нулевым разглашением позволяет сформировать систему, в которой каждая подсистема усиливает остальные. Постквантовая криптография обеспечивает устойчивость к перспективным вычислительным угрозам, пороговое хранение устраняет единую точку отказа, а аутентификация без передачи секрета снижает риск его утечки.

При этом данный подход требует дополнительных ресурсов: возрастают объёмы передаваемых данных, сложность протоколов и требования к реализации. Поэтому дальнейшие исследования должны быть направлены на оптимизацию производительности и экспериментальную оценку системы.

Таким образом, объединение постквантовой криптографии, пороговых схем распределения секрета и аутентификации на основе доказательства с нулевым разглашением позволяет построить децентрализованную систему конфиденциального хранения и аутентификации, ориентированную на противодействие современным и перспективным угрозам.

Литература

1. P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in Proc. 35th Annu. Symp. Foundations of Computer Science (FOCS), Santa Fe, NM, USA, Nov. 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.
2. N. K. Chistousov, I. A. Kalmykov, D. V. Dukhovnyj, M. I. Kalmykov, and A. A. Olenov, “Adaptive Authentication Protocol Based on Zero-Knowledge Proof,” Algorithms, vol. 15, no. 2, p. 50, 2022, doi: 10.3390/a15020050.
3. J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, “CRYSTALS–Kyber: A CCA-Secure Module-Lattice-Based KEM,” IACR Cryptol. ePrint Arch., Rep. 2017/634, 2017.
4. A. Langlois and D. Stehle, “Worst-Case to Average-Case Reductions for Module Lattices,” Cryptology ePrint Archive, Paper 2012/090, 2012.
5. A. Shamir, “How to share a secret” Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

DEVELOPMENT OF A SECURE SYSTEM FOR KEY TRANSMISSION AND STORAGE USING POST-QUANTUM CRYPTOGRAPHY AND THRESHOLD SCHEMES

student Baranova E.I.¹, Assoc. Professor Butakova N.G.^{1,2}, student Vinnik E.A.¹, student Filippova P.V.¹

¹Moscow Polytechnic University

²National Research University of Electronic Technology

In the context of the development of quantum computing technologies, there is a need to improve secure key transmission systems. The use of classical cryptographic algorithms becomes insufficiently reliable due to their vulnerability to quantum attacks. In this work, the architecture of a secure key transmission system is considered, including post-quantum key exchange, authentication based on zero-knowledge proofs, and distributed storage using threshold schemes. The proposed approach is aimed at increasing the cryptographic strength and fault tolerance of the system under modern and prospective threats.



АНАЛИЗ СУЩЕСТВУЮЩИХ ПОДХОДОВ К ОЦЕНКЕ УРОВНЯ ЗРЕЛОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

асп. Быков А.И., студ. Облиенко А.В.

Национальный исследовательский университет «МИЭТ»

В условиях беспрецедентного роста киберугроз и цифровой трансформации экономики, оценка уровня зрелости информационной безопасности (ИБ) организации перестала быть вспомогательной задачей и превратилась в стратегическую функцию управления. Для практических специалистов выбор инструментария для такой оценки представляет собой сложную дилемму, обусловленную сосуществованием двух фундаментально разных парадигм: риск-ориентированных международных стандартов и директивных отечественных регуляторных требований. В статье представлен аналитический обзор и проводится сопоставление ключевых подходов к оценке зрелости ИБ организации. Анализ фокусируется на их концепциях, практической применимости, а также на системных ограничениях, с которыми сталкиваются специалисты при их внедрении. На основе проведенного исследования делается вывод о практической применимости моделей. Предлагается стратегия интеллектуального синтеза – использование обязательных требований как базового уровня соответствия, дополняемого элементами международных фреймворков для повышения адаптивности, устойчивости и реальной защищенности организации. Целью такой гибридной стратегии должно стать не формальное соответствие, а достижение подлинной зрелости ИБ организации, способной противостоять динамично меняющемуся ландшафту киберугроз.

В мире цифровой трансформации экономики и роста киберугроз обеспечение информационной безопасности (ИБ) организации перестает быть исключительно технической задачей и превращается в одну из стратегических функций управления. Для правильного распределения ресурсов и демонстрации готовности организациям необходимы качественные инструменты для оценки состояния своей защиты в реальном времени. На международном уровне есть множество подходов к такой оценке. Для специалистов по управлению информационной безопасностью выбор и применение этих подходов представляет собой тяжелую задачу, которая требует понимания их структуры и ограничений.

Понятие информационная безопасность является многогранным и может трактоваться по-разному в зависимости от контекста. В общем смысле под информационной безопасностью понимается состояние защищенности информации при котором обеспечены её конфиденциальность, доступность и целостность [1]. Это состояние достигается путем защиты информации на всех этапах ее жизненного цикла – от создания до уничтожения [2, 3].

Однако, для целей оценки зрелости процессов информационной безопасности необходимо более детальное определение. Международные подходы, в частности семейство стандартов ISO/IEC¹ 27000, рассматривают ИБ² через призму системы управления информационной безопасностью. В этом контексте содержание ИБ – это не просто набор технических средств, а совокупность взаимосвязанных процессов: разработка политики, управление рисками, выбор и внедрение контрмер, мониторинг, аудит и непрерывное улучшение. Такой подход делает ИБ динамичной и адаптивной, ориентированной на бизнес-цели и меняющиеся риски.

Целостная зрелость представляет собой уровень ИБ, при котором безопасность встроена в продукты, услуги, и процессы организации, а устойчивость обеспечивается не только внутренними мерами, но и совместными действиями с клиентами и партнерами.

На нормативном уровне информационная безопасность определяется как состояние защищенности от угроз. В Доктрине информационной безопасности Российской Федерации закреплено: «Информационная безопасность Российской Федерации – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [4]. Несмотря на масштаб формулировки, ключевой элемент – состояние защищенности – сохраняет актуальность и на уровне отдельной организации.

В национальном стандарте ГОСТ³ Р ИСО/МЭК 27000-2021 дано более прикладное определение: «информационная безопасность – сохранение конфиденциальности, целостности и доступности информации» [5].

Российское законодательство и регуляторные акты часто определяют ИБ более статично [6]. Например, в контексте объектов критической информационной инфраструктуры (КИИ) безопасность рассматривается как состояние защищенности, достигаемое выполнением конкретного перечня организационных и

¹ ISO/IEC – International Organization for Standardization / International Electrotechnical Commission

² ИБ – информационная безопасность

³ ГОСТ – Государственный стандарт

технических мер, предписанных нормативными документами ФСТЭК России⁴. Здесь содержание ИБ сводится к соблюдению установленных процедур и использованию необходимых средств защиты. Такой подход обеспечивает единообразие и прозрачность, но иногда может быть менее гибким в ответ на новые, неописанные ранее угрозы.

Данные характеристики образуют фундамент классической модели ИБ, однако для анализа объекта необходимо расширенное толкование. Под объектом информационной безопасности в рамках настоящего исследования понимается организация либо её функциональный сегмент, включающий информационные активы, программно-технические средства, инфраструктуру, а также персонал, вовлечённый в информационные процессы. Рассматриваемый отечественный подход фокусируется на защите конкретного объекта (ОКИИ⁵, ИСПДн⁶), а не на общей модели безопасности всей организации.

Таким образом, уже на концептуальном уровне закладываются различия в рассматриваемых методологиях оценки: международные фокусируются на процессах и управлении, отечественные – на выполнении контрмер и соответствии требованиям к объектам информатизации.

Модели зрелости процессов ИБ представляют собой структурированные подходы, позволяющие организациям оценивать текущее состояние своих процессов ИБ и определять пути их улучшения. Они обычно предполагают наличие нескольких уровней (например, от начального до оптимизируемого), каждый из которых характеризуется определенным набором атрибутов и практик. Применение таких моделей позволяет выявить сильные и слабые стороны, установить приоритеты для инвестиций и отслеживать прогресс во времени.

Наиболее распространенными на мировом уровне являются четыре основные модели: NIST Cybersecurity Framework (CSF)⁷, серия стандартов ISO/IEC 27000, COBIT⁸ и CMMI⁹. Эти модели различаются по своей структуре, целям и степени формализации. NIST CSF предлагает функциональный подход, разделяя деятельность на пять ключевых функций: Идентификация, Защита, Обнаружение, Реагирование и Восстановление. ISO/IEC 27001 задает формальные требования к созданию и поддержанию системы управления ИБ, основанной на цикле PDCA¹⁰. COBIT фокусируется на корпоративном управлении ИТ и обеспечении соответствия ИБ-стратегии бизнес-целям. CMMI, изначально созданная для оценки зрелости процессов разработки программного обеспечения, предлагает пятиуровневую шкалу для количественной оценки зрелости любых процессов, включая ИБ.

Выбор модели зависит от стратегических целей организации. Для коммуникации с руководством и быстрой оценки рисков подходит NIST CSF. Для получения международного признания и сертификации – ISO/IEC 27001. Для выстраивания вертикального управления ИТ – COBIT. Для количественного измерения зрелости процессов – CMMI. На практике многие организации используют гибридные подходы, комбинируя элементы разных моделей для достижения максимальной эффективности.

ISO/IEC 27001 является глобальным стандартом для сертификации систем управления ИБ. Его главная задача – предоставление четкой, структурированной и признаваемой во всем мире основы для построения системы управления ИБ. Процесс сертификации включает независимый аудит, что придает полученному статусу высокий авторитет и служит маркетинговым преимуществом для организаций, работающих на международном рынке. Однако этот подход требует значительных ресурсов и времени, что может быть непосильно для малого и среднего бизнеса. Существует довольно коварный феномен, который именуют «парадоксом сертификации». Ситуация, на первый взгляд, абсурдная: организация блестяще проходит аудит, её папки ломятся от безупречных документов, процедуры выверены до запятой – и всё это создает иллюзию абсолютной защищенности. Однако, за этим фасадом бумажного благополучия часто скрываются уязвимости. Так происходит, потому что аудит проверяет соответствие формальным критериям здесь и сейчас. Хотя, возможно, дело лишь в методологических пробелах современных стандартов. Так или иначе, наличие сертификата вовсе не гарантирует защищенность: можно иметь все необходимые документы, подписанные уполномоченными лицами, и при этом оставаться беззащитным перед атакой, которую эти самые документы даже не предусматривают.

⁴ ФСТЭК России – Федеральная служба по техническому и экспортному контролю

⁵ ОКИИ – Объект критической информационной инфраструктуры

⁶ ИСПДн – информационные системы персональных данных

⁷ NIST CSF – NIST Cybersecurity Framework / Рамка кибербезопасности Национального института стандартов и технологий США

⁸ COBIT – Control Objectives for Information and Related Technologies / Цели управления информацией и смежными технологиями

⁹ CMMI – Capability Maturity Model Integration / Интегрированная модель зрелости процессов

¹⁰ PDCA – Plan-Do-Check-Act / Планирование–Действие–Проверка–Совершенствование

NIST Cybersecurity Framework (CSF) представляет собой функциональную модель, разработанную Национальным институтом стандартов и технологий США. Его структура построена вокруг пяти основных функций: Identify (Идентификация), Protect (Защита), Detect (Обнаружение), Respond (Реагирование) и Recover (Восстановление). Внутри каждой функции скрывается множество из подфункций и категорий – деталей, которые помогают организации не просто описать свою деятельность, а осмыслить её. И вот здесь кроется главная особенность фреймворка, его своеобразная «сила» – гибкость. Это не жесткий стандарт, загоняющий всех в сертификацию, это скорее инструкция по эксплуатации сложного механизма. Организация сама решает, какие процессы и технологии внедрять, исходя из собственных рисков и специфики деятельности. Вторая версия стандарта сделала этот инструмент еще более гибким, добавив практические руководства по достижению зрелости, что, безусловно, шаг вперед, хотя и не лишенный своих нюансов.

COBIT – модель корпоративного управления ИТ¹¹ от ISACA¹² - представляет собой нечто большее, чем просто свод правил; это, пожалуй, одна из самых известных международных концепций, которая сознательно выходит за узкие рамки технической информационной безопасности. Её фокус смещен туда, где часто возникает недопонимание: на управление в целом и обеспечение соответствия в масштабах всей ИТ-инфраструктуры организации. Главная идея, заключается в построении прочного, почти неразрывного моста между стратегией кибербезопасности и глобальными бизнес-целями организации. Ведь без этого связующего звена любые усилия специалистов рискуют стать дорогими, но бесполезными. Модель предлагает структурированный, даже педантичный набор принципов, процессов и метрик. Чтобы эффективно распоряжаться ИТ-ресурсами, минимизировать риски и, что критически важно, не выпасть из поля зрения регуляторов. Хотя COBIT, как и многие другие современные подходы, не является стандартом для прямой сертификации, он содержит изящные механизмы оценки зрелости процессов. Это позволяет организациям не гадать, а объективно измерять свой прогресс, выявляя те самые «слепые зоны», где требуются улучшения. Для специалистов по ИБ, работающих в громоздких корпоративных структурах, COBIT становится буквально незаменимым инструментом убеждения: он помогает продемонстрировать реальную ценность информационной безопасности для организации.

Параллельно с этим нельзя не упомянуть CMMI. Эта модель предлагает строго количественный подход к оценке зрелости. Здесь речь идет не о субъективных заявлениях, а о возможности измерять уровень развития и отслеживать динамику через числовые показатели. Подобный прагматизм особенно полезен для проектных офисов и команд разработки, где от тебя требуют доказать предсказуемость процессов и гарантированное качество результата – слова тут мало что значат, нужны цифры.

Однако, и здесь возможно позволить себе долю скепсиса, даже самые гибкие и продуманные модели, будь то NIST CSF или SAMM¹³, редко могут предложить действительно эффективный механизм предварительного профилирования организации. Они, словно по умолчанию, рассчитывают, что зрелость можно и нужно оценивать с чистого листа, игнорируя исходный масштаб бизнеса или его уникальную модель. Стоит учесть, что универсальность часто оборачивается потерей нюансов, а каждая организация, в конце концов, уникальна в своих проблемах.

Проведенный анализ подводит нас к довольно прозаичному, но неизбежному выводу: современные модели зрелости информационной безопасности, при всей их несомненной методологической ценности, изначально «заточены» под узкие, специфические цели и контексты. Возьмем, к примеру, международные фреймворки вроде NIST CSF или ISO/IEC 27001. Да, они предлагают завидную гибкость и глубокую ориентацию на бизнес-риски, но они существуют в вакууме, игнорируя законодательные требования по ИБ, которые обязательны для отечественных компаний. Более того, нельзя закрывать глаза на то, что у каждой из этих методик есть свои внутренние проблемы – проблемы внедрения, которые часто недооцениваются на старте.

Таким образом, картина вырисовывается следующая: ни одна из современных моделей – будь то гибкий и адаптивный NIST CSF, структурированный ISO/IEC 27001 или количественный CMMI – не способна в одиночку обеспечить реальную защищенность организации. Мы живем в условиях сложнейшего ландшафта угроз, где переплетаются регуляторные требования и постоянно развивающиеся киберугрозы. Эти фреймворки, безусловно, ценны, они служат отличными инструментами для управления, планирования и, что немаловажно, для коммуникации между техническими специалистами и руководством организации. Однако, и здесь можно быть категоричным, они не заменяют собой регуляторные требования Российской

¹¹ ИТ – Информационные технологии

¹² ISACA – Information Systems and Control Association / Ассоциация аудита и контроля информационных систем

¹³ SAMM – Software Assurance Maturity Model / Модель зрелости обеспечения безопасности программного обеспечения.

Федерации. Они не учитывают, да и не могут учитывать в полной мере, специфику отечественного правового поля со всеми его нюансами. Слепое следование западной методике без оглядки на локальное законодательство – это путь в никуда, где формальная «зрелость» процесса может обернуться реальной уязвимостью перед требованиями государства.

Для отечественных организаций, особенно тех, что работают в стратегических отраслях, игнорирование требований ФСТЭК России, ЦБ РФ¹⁴ и федеральных законов – это не просто риск получить штраф, это прямая угроза приостановки деятельности. Поэтому подлинная зрелость информационной безопасности достигается не через слепой выбор одной «самой правильной» методологии, а через их осознанный синтез. Нужно уметь совмещать несовместимое: международные стандарты и регуляторные требования, создавая гибридную систему защиты, которая работает и на бумаге, и в реальности. Хотя, возможно, такой путь требует куда больше ресурсов, чем кажется на первый взгляд.

Литература

1. ГОСТ Р 53114-2008 // CNTD. URL: <https://docs.cntd.ru/document/1200075565> (дата обращения 07.04.2026).
2. Kochedykov S.S., Grechishnikov E.V., Dushkin A.V., Orlova D.E. The mathematical model of cyber attacks on the critical information system. Journal of Physics: Conference Series, Voronezh. Vol. 1202. Voronezh: Institute of Physics Publishing, 2019. Pp. 12013. DOI 10.1088/1742-6596/1202/1/012013.
3. Кочедыков С.С., Душкин А.В., Новосельцев В.И., Соколовский С.П. Моделирование системы конфликтных взаимодействий в информационной системе критического применения // Вестник Воронежского института ФСИИ России. – 2017. – № 4. – С. 74-84.
4. Доктрина информационной безопасности РФ // Совет безопасности РФ. URL: <http://www.scrf.gov.ru/security/information/document5/> (дата обращения 07.04.2026).
5. ГОСТ Р ИСО/МЭК 27000-2021 // Электронный фонд правовых и нормативно-технических документов. URL: <https://docs.cntd.ru/document/1200179675/> (дата обращения 07.04.2026).
6. Методика оценки уровня зрелости Информационной безопасности компании // Sberbank. URL: <https://www.sberbank.ru/ru/person/kibrary/experts/metodika-ocenki-urovnya-zrelosti-kiberbezopasnosti-fokusnykh-kompanij-gruppy-pao-sberbank/> (дата обращения 07.04.2026).

ANALYSIS OF EXISTING APPROACHES TO ASSESSING THE INFORMATION SECURITY MATURITY LEVEL OF ORGANIZATIONS

postgrad. stud. Bykov A.I., Obliencko A.V.

National Research University of Electronic Technology

In the context of the unprecedented growth of cyber threats and the digital transformation of the economy, assessing an organization's information security (IS) maturity level has ceased to be a secondary task and has become a strategic management function. For practitioners, choosing the right tools for such assessment presents a complex dilemma due to the coexistence of two fundamentally different paradigms: risk-based international standards and prescriptive Russian regulatory requirements. This article presents an analytical review and compares key approaches to assessing an organization's IS maturity. The analysis focuses on their concepts, practical applicability, and the systemic limitations faced by professionals during their implementation. Based on the conducted research, a conclusion is reached on the practical applicability of the models. An intelligent synthesis strategy is proposed – using mandatory requirements as a baseline level of compliance, supplemented by elements of international frameworks to improve the adaptability, resilience, and actual security of the organization. The goal of such a hybrid strategy should not be formal compliance, but rather achieving genuine IS maturity within the organization, capable of withstanding the dynamically changing cyber threat landscape.



¹⁴ ЦБ РФ – Центральный банк Российской Федерации

МЕТОД СЦЕНАРНОГО ПРОГНОЗИРОВАНИЯ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ, ПОДВЕРЖЕННЫХ КИБЕРАТАКАМ

доц. Воеводин В.А., студ. Виноградов И.В.

Национальный исследовательский университет «МИЭТ»

Предложен метод прогнозирования устойчивости объектов информатизации (ОИ), основанный на интеграции полумарковских процессов смены состояний элементов ОИ и антагонистической игры сторон с ограниченными ресурсами, борющихся за контроль над количественным показателем устойчивости. Новизна заключается в переходе от статического анализа защищенности ОИ к сценарному моделированию кибератаки, что дает инженерно интерпретируемые метрики устойчивости в динамике. Эксперимент показал: информированность атакующего о структуре ОИ ведет к превышению целевого времени восстановления (RTO); при отсутствии информации защищающиеся удерживают показатель в допустимых пределах. Результаты работы могут быть использованы для количественного обоснования распределения ресурсов защиты, а также при создании тренажерных комплексов для подготовки специалистов по кибербезопасности. Разработанная модель создает основу для дальнейшего применения методов искусственного интеллекта с целью поиска оптимальных стратегий противоборства сторон.

Введение. При проектировании и эксплуатации объектов информатизации (ОИ) традиционные методы оценки надежности, основанные на статистике отказов [1, 2], неприменимы для анализа нештатных ситуаций, вызванных кибератаками, так как не учитывают нестационарный характер критических событий и адаптивное поведение источника киберугроз [3]. Теория игр позволяет моделировать киберконфликты [4, 5], но оперирует на высоком уровне абстракции, что не позволяет соотнести полученные стратегии с физической топологией сети ОИ и бюджетом ресурсов защиты.

Для решения практической задачи обеспечения устойчивости ОИ необходим синтез этих подходов, позволяющий прогнозировать устойчивость как результат динамического противоборства. Целью работы является разработка метода прогнозирования устойчивости на основе интеграции:

- а) полумарковских процессов смены состояний элементов ОИ, подверженных кибератаке;
- б) антагонистической игры для учета стратегий атаки и защиты;
- в) ограничений по ресурсам сторон.

Новизна подхода заключается в операционализации игрового взаимодействия «защитник-атакующий» на графе сети ОИ, что позволяет перейти от абстрактных стратегий к инженерно интерпретируемым метрикам, включая вероятность сохранения функциональности и критический запас ресурсов защиты.

Постановка задачи. Для органов управления, ответственных за обеспечение кибербезопасности ОИ, ключевое значение имеет не только оценка текущего уровня его устойчивости, но и прогноз его изменения во времени.

Рассматривается ОИ, структура которого задана в виде совокупности элементов, объединенных единой целью в систему. В процессе функционирования система подвергается воздействию киберугроз. На этапах проектирования и эксплуатации для каждого элемента реализуется комплекс мер защиты, формирующих его индивидуальную защищенность. Совокупность этих мер определяет способность ОИ противостоять угрозам, характеризуемую устойчивостью системы [6]. Источник угроз, стремящийся дестабилизировать работу системы, реализует комплекс атакующих воздействий на ее элементы.

Для исследования устойчивости системы в условиях кибератаки используется динамическая модель, описывающая антагонистическое взаимодействие двух сторон: атакующей, заинтересованной в нарушении штатного режима функционирования ОИ, и защищающейся, обеспечивающей сохранение функциональности системы.

Предметом моделирования является динамика интегрального показателя устойчивости системы, определяемого показателями устойчивости отдельных элементов и топологией их связей. Целью атакующих является снижение данного показателя ниже критического порога с удержанием его в этом состоянии в течение времени, превышающего целевое время восстановления (Recovery Time Objective, RTO). Цель защищающихся — не допустить снижения показателя ниже порога либо обеспечить восстановление функциональности системы до допустимого уровня показателя устойчивости за время, не превышающее RTO.

Формально, структура системы представляется в виде простого графа. Состояние ОИ в дискретные моменты времени описывается набором матриц, отражающих текущий уровень защищенности элементов и их восстанавливаемость.

Стороны обладают ограниченными ресурсами. Атакующие распределяют ресурс на разведку, выбор целей и реализацию воздействий. Защищающиеся распределяют ресурс между превентивным усилением защищенности элементов и проведением восстановительных мероприятий после атак.

Динамика функционирования и деградации каждого элемента системы задаётся стохастической моделью (полумарковским процессом) [7], которая отражает действия обеих сторон.

Правила игры. Модель поддерживает различные форматы игры. В формате «блиц» на фиксированном временном горизонте атакующие побеждают, если снизят показатель устойчивости системы ниже порога и удержат его дольше RTO. В формате «на ресурс» игра идет до истощения ресурсов: если показатель устойчивости остался в допустимом промежутке, побеждает сторона, сохранившая ресурс.

Игра может проходить в нескольких режимах. В режиме «RTO» для победы атакующего требуется удержание показателя ниже порога дольше заданного RTO. В режиме «флаг» ($RTO = 0$) достаточно самого факта снижения. Ресурс сторон может быть либо только расходуемым, либо пополняемым (в формате «на ресурс» количество пополнений ограничено). В рамках одной и той же игры режимы расхода ресурса у сторон могут различаться.

Во всех форматах и режимах целевая функция одна — это функция устойчивости системы, контроль над которой и составляет суть противоборства. Так, модель позволяет исследовать влияние стратегий распределения ресурсов на динамику устойчивости.

Метод. Основным методом исследования выступает алгоритм прямого численного прогноза, основанный на последовательном расчете состояний полумарковских процессов для всех элементов системы. Метод позволяет для произвольных, но фиксированных стратегий сторон получить траекторию функции устойчивости системы на заданном временном горизонте. Алгоритм включает цикл по дискретному игровому времени от нуля до наступления условия завершения игры (задается, исходя из сценария и режима игры) с заданным шагом дискретизации времени (инкремент цикла); на каждой итерации, т.е. для каждого момента времени, выполняются шаги:

1. Применение стратегий.

Атакующий на основе своих знаний о системе и ресурса формирует деструктивные воздействия на элементы системы. Ресурс уменьшается на стоимость воздействий. Защитники применяют меры по усилению защищенности функционирующих элементов системы или по восстановлению их функциональности, если они были повреждены в результате воздействия атакующего. Ресурс защиты также уменьшается на стоимость выполненных мер.

2. Расчет вероятностных характеристик элементов.

Вероятность нахождения каждого элемента ОИ в функциональном состоянии определяется из системы интегральных уравнений (подробно выведена в [8]) и зависит от интенсивностей воздействия угрозы и восстановления, скорректированных на текущие ресурсы сторон.

3. Расчет функции устойчивости системы.

Полученные на шаге 2 значения агрегируются на основе структуры системы, а также статистических характеристик надежности элементов. В результате вычисляется значение глобальной функций устойчивости системы в следующий момент времени.

4. Проверка критерия завершения игры и переход к следующей итерации (шаг 1).

Моделирование и демонстрация игровой динамики. В настоящем разделе продемонстрирована работа метода и модели. Цель – показать, как уровень информированности атакующего влияет на динамику и исход игры. В настоящей демонстрации для наглядности влияния информированности стратегии сторон фиксированы. Поиск оптимальных стратегий – направление для следующего этапа исследований. Входные условия игры представлены таблицей 1. Характеристики защищенности элементов, – в таблице 2.

Таблица 1

Входные условия игры

Исходные данные	Описание
Формат игры	Блиц
Режимы игры	RTO, только расходуемый ресурс
Топология системы	Э1-Э2-Э3 (три последовательных элемента)
RTO	9 ч
Допустимый порог показателя устойчивости	0,4
Ресурс атакующего	150 у.е. (50 у.е. за одно воздействие)
Ресурс защиты	100 у.е. (30 у.е. за одно восстановление)

Таблица 2

Характеристики защищенности элементов

Элемент	Вероятность поражения	Характеристика надежности
Э1	0,2	0,95
Э2	0,7	0,99
Э3	0,1	0,9

Сценарий 1:

Атакующий не знает ни структуру системы, ни характеристики защищенности элементов. Поэтому, его стратегией является равновероятное последовательное воздействие по всем элементам. Осуществляет воздействия: по Э1 с 1 ч по 6 ч, по Э2 с 6 ч по 10 ч, по Э3 с 12 ч по 15 ч. При этом расходует весь ресурс. Защитник выполняет восстановительные работы поврежденных элементов: Э1 с 9 ч по 20 ч, Э2 с 7 ч по 11 ч, Э3 с 13 ч по 18 ч. При этом расходует 90 у.е. ресурса. Траектория показателя устойчивости этого сценария представлена на рисунке 1. Выигрывают защитники, потому что им удалось вернуть показатель в допустимый промежуток за 8 ч, что меньше RTO.

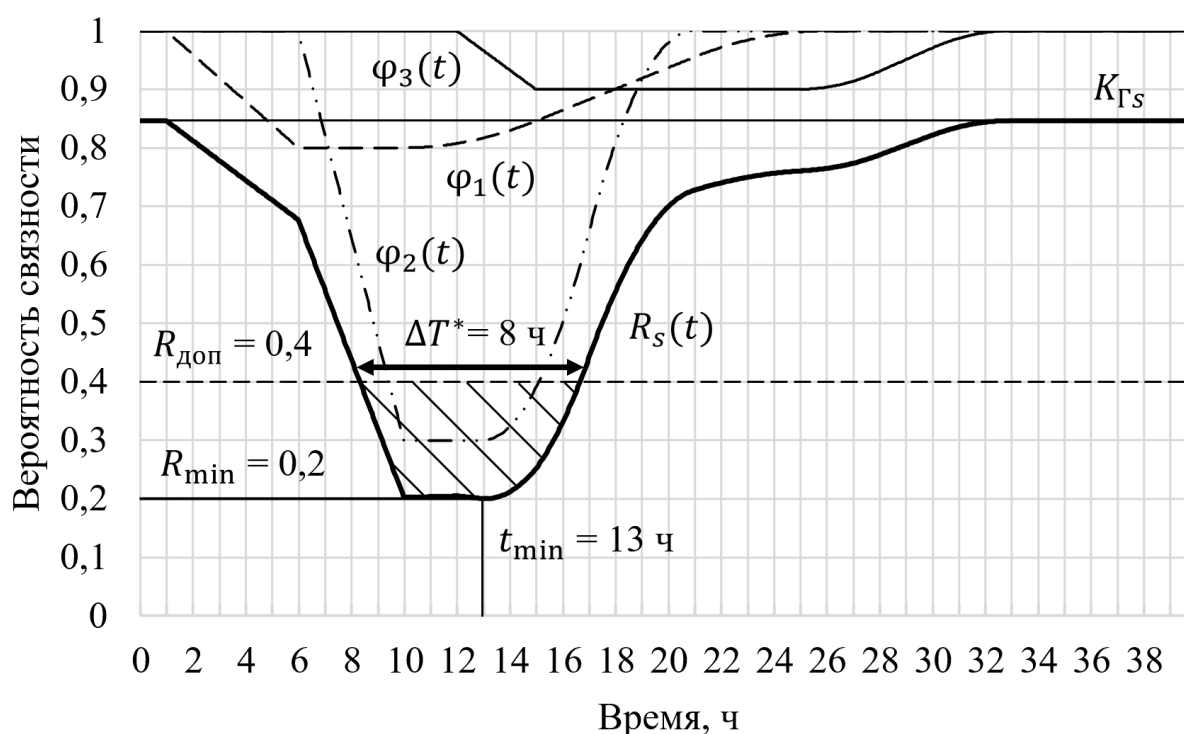


Рисунок 1 – Траектория устойчивости по сценарию 1

Сценарий 2:

Целенаправленная кибератака на слабое звено. Атакующий знает структуру и характеристики элементов. Его стратегия – сосредоточить силы на наименее защищенном элементе – Э2, потому что элемент последовательно связан с остальными и имеет наибольшую вероятность поражения. Осуществляет воздействия: по Э2 с 1 ч по 6 ч, по Э2 с 6 ч по 10 ч, по Э2 с 12 ч по 15 ч. При этом расходует весь ресурс. Защитник выполняет восстановительные работы поврежденных элементов: Э2 с 9 ч по 20 ч, Э2 с 7 ч по 11 ч, Э3 с 13 ч по 18 ч. При этом расходует 90 у.е. ресурса. Траектория показателя устойчивости этого сценария представлена на рисунке 2. Выигрывают атакующие, потому что в результате целенаправленного воздействия они снизили показатель устойчивости ниже порога и удержали его дольше RTO почти в 1,5 раза.

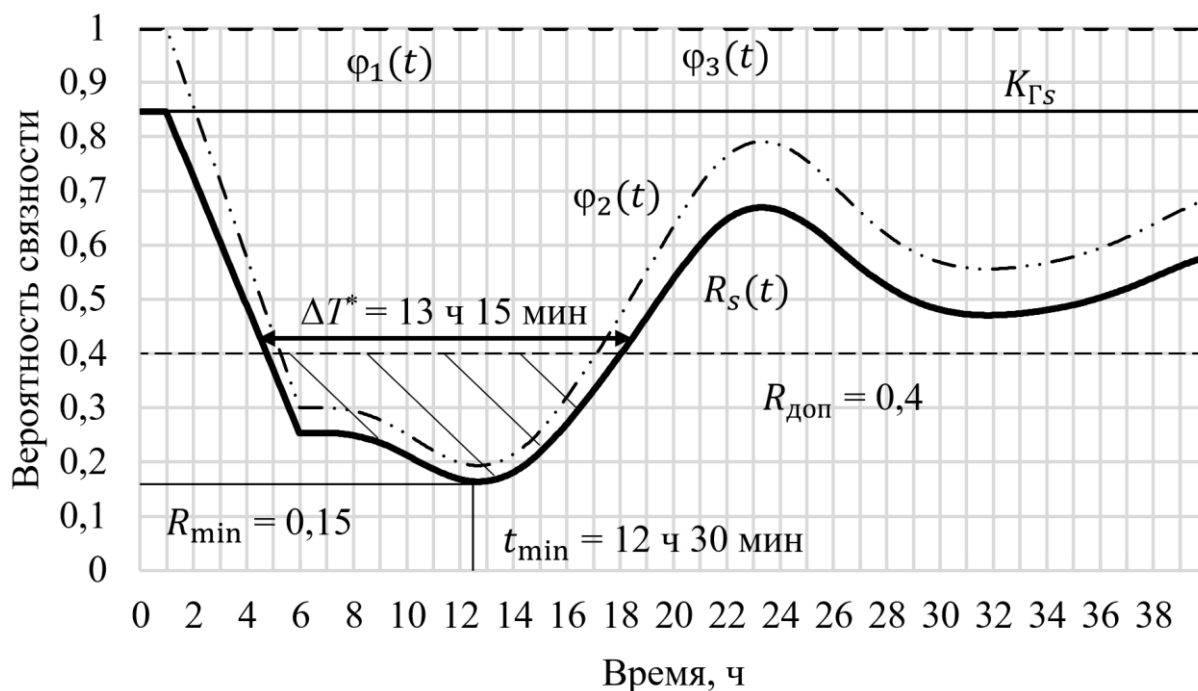


Рисунок 2 – Траектория устойчивости по сценарию 2

Выводы. В статье предложен метод, редуцирующий задачу оценки устойчивости сложных систем к анализу эволюции игрового поля. Экспериментально подтверждено, что метод позволяет адекватно отобразить ключевые аспекты антагонистического противостояния: значимость информационного преимущества атакующего и ресурсно-стратегический баланс сторон. Интегральный показатель устойчивости выступает количественным критерием исхода противоборства.

Практическая значимость работы заключается в создании основы для проактивного управления киберустойчивостью, количественного обоснования распределения ресурсов защиты и построения тренажерных комплексов для подготовки специалистов. Разработанная модель открывает перспективы применения методов искусственного интеллекта для поиска оптимальных стратегий и прогностической аналитики.

Основным ограничением версии модели является необходимость экспертной параметризации, что определяет направление дальнейших исследований. Предложенный подход направлен на преодоление разрыва между структурным анализом надежности и моделированием конфликтов.

Литература

1. Крылов Е.Г., Макаров А.М. Надежность технических систем. Методы расчета : учебное пособие / Е.Г. Крылов, А.М. Макаров. – Москва ; Вологда : Инфра-Инженерия, 2026. – 108 с.
2. Тимошенков С.П. Надежность технических систем и техногенный риск : учебник и практикум для вузов / С.П. Тимошенков, Б.М. Симонов, В.Н. Горощко. — 2-е изд., испр. и доп. – Москва : Издательство Юрайт, 2025. — 551 с. – (Высшее образование). – ISBN 978-5-534-19935-2.
3. Zhuang, J., & Bier, V. (2020). Validating Models of Adversary Behavior. CREATE, University of Southern California. – Режим доступа: <https://create.usc.edu/validating-models-of-adversary-behavior-2>, свободный (дата обращения: 30.03.2026).
4. He, F., J. Zhuang, N. Rao, C. Ma, and D. Yau. Game-Theoretic Resilience Analysis of Cyber-Physical Systems. First IEEE International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA 2013), Taipei, Taiwan, August 19-20, 2013. doi:10.1109/CPSNA.2013.6614252.
5. Бондаренко Б.П. Математическое моделирование задач информационной защиты с помощью теории игр / Б.П. Бондаренко // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2024. – № 6. – С. 35-39. – doi:10.37882/2223-2966.2024.06.06.
6. Язов Ю.К. Об определении понятия «кибербезопасность» и связанных с ним терминов / Ю.К. Язов // Вопросы кибербезопасности. – 2025. – № 1(65). – С. 2-6. – doi:10.21681/2311-3456-2025-1-2-6.

7. Воеводин В.А. Математическая модель оценивания устойчивости функционирования элемента информационной инфраструктуры автоматизированной системы управления, подверженной воздействию угроз информационной безопасности / В.А. Воеводин // Информационные технологии. – 2024. – Т. 30, № 1. – С. 23–31. – doi:10.17587/it.30.23-31.
8. Воеводин В.А. Об оценке устойчивости функционирования объекта информатизации в условиях компьютерных атак при экспоненциальном законе распределения времени до воздействия противника и восстановления работоспособности / В.А. Воеводин, И.В. Виноградов, Д.И. Волков // Вестник Дагестанского государственного технического университета. Технические науки. – 2022. – Т. 49, № 3. – С. 39-51. – doi:10.21822/2073-6185-2022-49-3-39-51.

A SCENARIO-BASED METHOD FOR FORECASTING THE RESILIENCE OF INFORMATION SYSTEMS SUSCEPTIBLE TO CYBER-ATTACKS

assoc. prof. Voevodin V.A., stud. Vinogradov I.V.

National Research University of Electronic Technology

A method for forecasting the resilience of information technology objects (ITO) is proposed. This method integrates semi-Markov processes of changing the states of ITO elements and the antagonistic game of resource-constrained parties competing for control over a quantitative resilience metric. The novelty lies in the transition from static analysis of ITO security to scenario-based cyberattack modeling, which yields dynamic resilience metrics that can be interpreted by engineers. The experiment demonstrated that attackers' awareness of the ITO structure leads to exceeding the recovery time objective (RTO); without this information, defenders maintain the RTO within acceptable limits. The results of this study can be used to quantitatively justify the allocation of defense resources, as well as to create simulation systems for training cybersecurity specialists. The developed model provides a foundation for the further application of artificial intelligence methods to find optimal strategies for adversarial conflicts.



ЭКСПЛУАТАЦИОННАЯ ПРОВЕРКА МЕТОДИКИ АУДИТА АППАРАТНЫХ ПЛАТФОРМ ДЛЯ СРЕДСТВ ДОВЕРЕННОЙ ЗАГРУЗКИ

студ. Габеркорн А.Э.

Национальный исследовательский университет «МИЭТ»

Защита персональных данных (ПДн) регулируется Федеральным законом №152-ФЗ и Постановлением Правительства РФ №1119. Для ИСПДн уровней защищенности 1 и 2 модель угроз требует учета угроз, связанных с недекларируемыми возможностями аппаратного и программного обеспечения. Требования конкретизируются в Приказе ФСТЭК России №21. Особое внимание уделяется этапу загрузки системы, где критически важно отсутствие скрытых каналов модификации кода на уровне базовой системы ввода-вывода (BIOS/UEFI).

Средства доверенной загрузки (СДЗ) проверяют целостность аппаратной части и программного обеспечения, используют криптографические алгоритмы и блокируют загрузку с внешних носителей. Однако безопасность СДЗ зависит от защищенности underlying hardware platform. Угрозы включают несанкционированный доступ через уязвимости микропрограммного обеспечения компонентов, способных инициировать перепрошивку: центральный процессор, контроллеры управления (BMC), сетевые адаптеры. Целью работы является эксплуатационная проверка методики аудита аппаратных платформ для оценки их пригодности к эксплуатации в составе СКЗИ.

Одной из главных задач обеспечения информационной безопасности является контроль целостности аппаратных платформ, используемых в составе средств криптографической защиты информации (СКЗИ). Защита персональных данных (ПДн) регулируется Федеральным законом №152-ФЗ и требует учета особенностей информационных систем персональных данных (ИСПДн). Уровень защищенности ИСПДн определяется с учетом типов угроз, среди которых особое место занимают угрозы, связанные с недекларируемыми возможностями аппаратного и программного обеспечения. Для защиты применяются меры, описанные в требованиях ФСТЭК и ФСБ России. Особое внимание уделяется этапу загрузки системы, где эффективным средством защиты выступает средство доверенной загрузки (СДЗ). Однако перед внедрением СДЗ необходимо убедиться в отсутствии скрытых каналов модификации кода загрузки на уровне базовой системы ввода-вывода (BIOS/UEFI).

Принцип работы СДЗ заключается в проверке целостности аппаратной части и программного обеспечения, использовании криптографических алгоритмов и блокировке загрузки с внешних носителей.

Тем не менее, эффективность данных средств напрямую зависит от безопасности аппаратной платформы. Одной из главных угроз информационной безопасности является несанкционированный доступ к информации через уязвимости микропрограммного обеспечения. Под угрозой оказываются компоненты, способные инициировать перепрошивку: центральный процессор, контроллеры управления (BMC), сетевые адаптеры. Чтобы определить, как происходит защита на этапе загрузки, выделим основные этапы аудита. Методология включает получение материалов по продукту от производителя, составление перечня комплектаций платформы и анализ достаточности предоставленных материалов.

Для обеспечения безопасности важно не только определить тип угроз, но и внедрить комплекс защиты, который способен отразить атаку на всех этапах работы информационной системы. Особое внимание стоит уделить начальному этапу запуска системы, так как существует вредоносное программное обеспечение, которое функционирует до загрузки операционной системы на уровне BIOS либо UEFI. Угрозы связаны с недекларируемыми возможностями в системном ПО, закладками в прикладном ПО и внешними атаками. Для защиты применяются меры, описанные в приказе ФСТЭК России №21.

В ходе эксплуатационной проверки методики было выполнено комплексное исследование программного обеспечения BIOS. Целью анализа являлась проверка отсутствия у исследуемой аппаратной платформы возможностей по реализации деструктивных воздействий на загружаемое ПО и разработка рекомендаций по защите от их влияния. На выходе предоставляется перечень материалов, включающий отчет по результатам исследований, техническое задание, электрические и функциональные схемы, перечень компонентов с характеристиками, спецификации на компоненты, а также директории со считанными прошивками BIOS, BMC, LAN, RAID и результатами исследований. Проведение анализа ПО BIOS состоит из следующих этапов: получение материалов по продукту от производителя, составление полного исчерпывающего перечня комплектаций аппаратной платформы и исполнений платформы, анализ достаточности предоставленных материалов. Подготовка отчетных материалов включает формирование носителя, содержащего отчет и архив с материалами, техническое задание и распечатанный отчет.

В ходе исследования выполняется поиск следующих опасных функциональных возможностей: передача управления нештатной операционной системе, изменение параметров работы аппаратной платформы, нарушение штатного функционирования СВТ, возможность перепрограммирования микросхемы с компонентами ПО BIOS, возможность загрузки EFI-файла из Boot menu, возможность нештатного извлечения аппаратного модуля доверенной загрузки из состава аппаратной платформы, возможность сброса настроек BIOS, возможность

удаленного управления платформой. Для нейтрализации данных угроз применяются методы защиты, включающие установку пароля на вход в настройки BIOS, контроль загрузочного устройства с помощью СДЗ и опечатывание корпуса платформы.

Важным этапом является снятие защиты ПЗУ BIOS. ПЗУ делится на четыре уровня защиты от записи: получение доступа к ПЗУ в чипсете путём выставления значения регистра чипсета, изменение описания прав доступа к регионам на микросхеме ПЗУ, выставление значений регистров самих микросхем ПЗУ, обесточивание определённого вывода микросхемы ПЗУ. Для получения доступа на запись к ПЗУ необходимо выставить значение регистра чипсета BIOS_CNTL (BIOS Control Register). Он расположен по адресу 0xDC. Для изменения доступа SMM используются биты 0, 1, 5.

Бит 0 - BIOS Write Enable (BIOSWE). При значении 0 запись в ПЗУ запрещена (разрешено только чтение), при значении 1 запись разрешена. Если значение этого бита изменяется с 0 на 1, и бит 1 (BLE) установлен в 1, генерируется SMI-прерывание.

Бит 1 - BIOS Lock Enable (BLE). При значении 0 изменение бита 0 (BIOSWE) с 0 на 1 не генерирует SMI-прерывание. При значении 1 - генерируется SMI-прерывание. Если данный бит выставлен в 1, очистить (выставить в 0) его можно только сигналом PLTRST# (Platform Reset).

Бит 5 - SMM BIOS Write Protect Disable (SMM_BWP). При значении 0 запись в ПЗУ происходит независимо от того, находятся процессоры в режиме SMM или нет. При значении 1 запись производится только при условии, что все процессоры находятся в режиме SMM.

Проверено отсутствие конструкций, реализующих перепрограммирование микросхемы BIOS данными из внешних портов, модификацию кода AddOn ROM при затенении в ОЗУ, модификацию блоков микрокода процессора (проверка вызова wrmsr с ECX=79h, EDX=0), передачу управления на код из портов ввода/вывода, несанкционированную запись в накопители.

Для платформ с процессором Intel проведен анализ технологии DCI (Direct Connect Interface) с помощью инструмента CHIPSEC (модуль common.debugenabled). Статус PASSED соответствует заблокированному состоянию интерфейсов отладки. Выполнен анализ региона Intel Management Engine (ME). С помощью утилит UEFITool (рисунок 1) и ME Analyzer исследован бинарный файл BIOS, составлен список разделов IME.

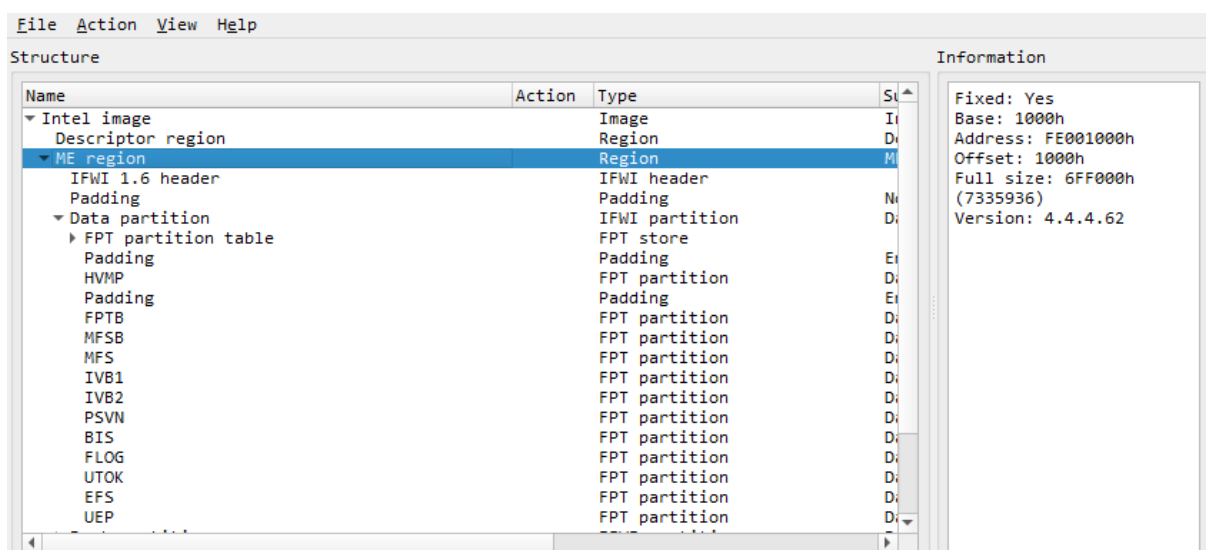


Рисунок 1. Использование UEFITool для определения разделов IME

Проверена возможность удаленного управления (Intel AMT). Выполнено сканирование портов утилитой Nmap (Zenmap). Критические порты AMT: 623 (ASF-RMCP), 664 (DMTF), 5900 (AMT VNC), 16992–16995 (AMT веб-серверы и редиректы) – не должны быть обнаружены (рисунок 2).

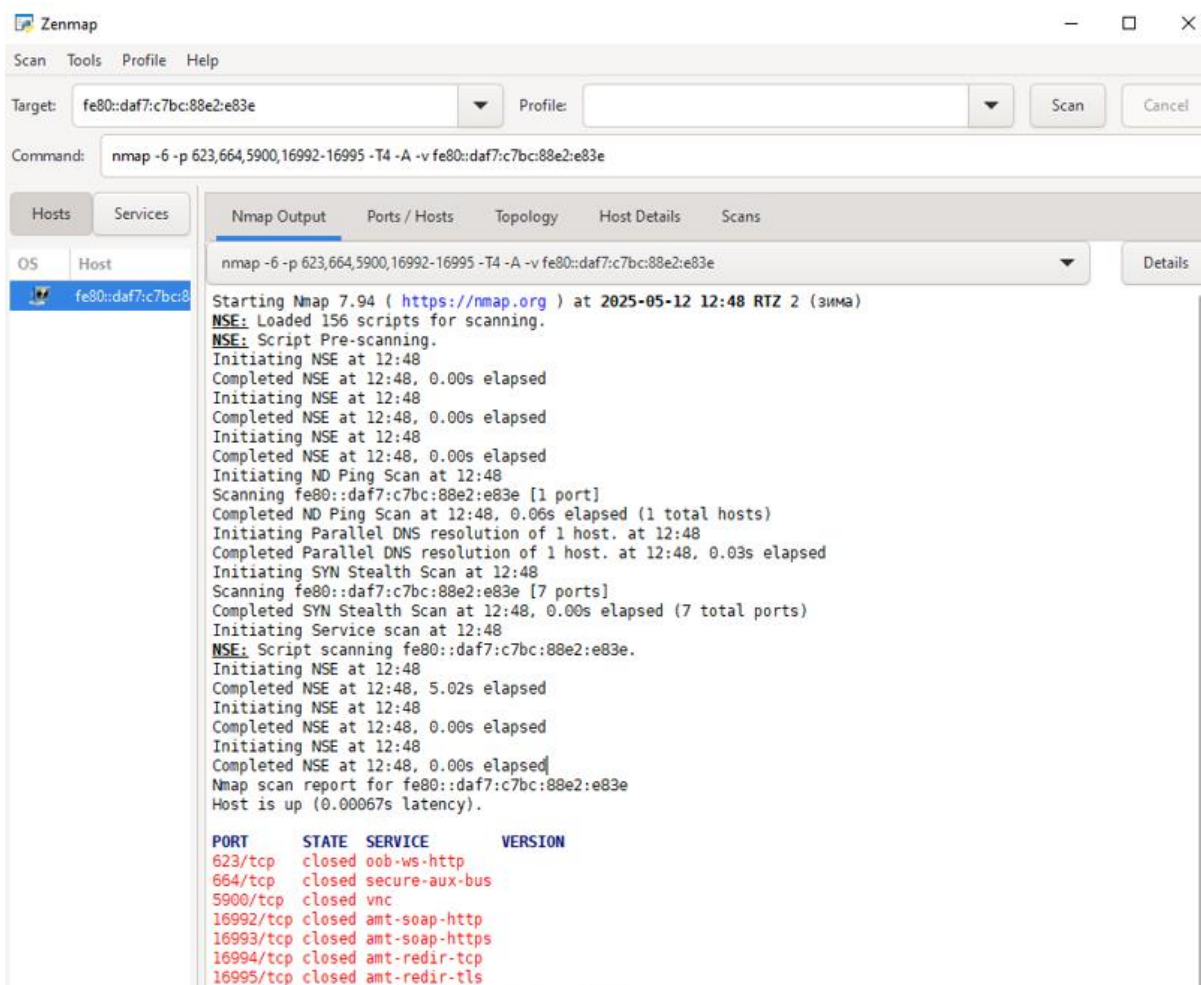


Рисунок 2. Nmap scan IPv6

При обнаружении открытых портов на интерфейсе management port делается вывод о возможности удаленного управления. Для нейтрализации угроз рекомендуется опечатывание порта и отключение функций в BIOS.

Проверена возможность входа в консоль U-BOOT (прерывание загрузки), наличие predefined пользователей (например, sysadmin). Доступ к консоли BMC возможен через 4-контактный разъем на материнской плате. Считана прошивка контроллера RAID, определена версия пакета обновления (утилита storcli.efi). Проанализирована структура образа (регионы OROM, Firmware). Проанализированы файлы прошивок сетевых контроллеров (например, Intel X710). Проверена структура NVM (области EMP, OROM, VPD).

Проверена поддержка протоколов NC-SI, MCTP и функции Bypass mode. Проверка NC-SI включает поиск информации в документации, аппаратную проверку линий, проверку параметров BIOS/UEFI. Проверка MCTP включает наличие демона mctpd в BMC, драйверов в ОС хоста. Проверка Bypass включает наличие реле на схеме адаптера, флагов в драйвере (ethtool).

В ходе эксплуатационной проверки методики выполнено комплексное исследование программного обеспечения BIOS и сопутствующих контроллеров. Все представленные в методике этапы соответствуют требованиям законодательства РФ о защите персональных данных и безопасности СКЗИ. Это предоставляет организациям возможность выбирать рациональные средства защиты, соответствующие необходимому уровню безопасности для конкретных информационных систем. Предложенная методика аудита аппаратных платформ разработана на основе требований регуляторов и практик проведения тематических исследований СКЗИ. Она не заменяет сертификационные испытания, но позволяет верифицировать готовность аппаратной платформы к эксплуатации криптографических средств требуемого класса. При использовании проверки механизмов защиты прошивок от несанкционированной записи идентифицируются все компоненты, способные инициировать перепрошивку: центральный процессор, контроллеры BMC, сетевые адаптеры. Цель - исключить скрытые каналы модификации кода доверенной загрузки. Выявляются компоненты, расширяющие поверхность атаки: коммутаторы Ethernet, функции Bypass, PXE в OPRM, контроллеры BMC с интерфейсами IPMI и NC-SI, модули TPM. Для каждого компонента определяются меры нейтрализации: исключение из спецификации закупки, физическая изоляция, программное отключение. Таким образом, методика позволяет подтвердить готовность

аппаратной платформы к эксплуатации СКЗИ требуемого класса без проведения дополнительных испытаний самой платформы, при условии неизменности компонентной базы и сохранения настроек безопасности.

Литература

1. Федеральный закон №152-ФЗ «О персональных данных».
URL: http://www.consultant.ru/document/cons_doc_LAW_66934/
2. Постановление Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». URL: http://www.consultant.ru/document/cons_doc_LAW_77397/
3. Приказ ФСТЭК России №21 - Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных.
URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21>
4. Документ Р 1323565.1 - Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации.
URL: <https://rst.gov.ru:8443/file-service/file/load/1699451272713>
5. Научная статья от академии Selectel - Что такое средства доверенной загрузки (СДЗ) и как они применяются.
URL: <https://selectel.ru/blog/what-is-sdz/>
6. UEFI Forum - UEFI Specification.
URL: <https://uefi.org/specifications>
7. CHIPSEC Framework - Platform Security Assessment Framework.
URL: <https://github.com/chipsec/chipsec>
8. Intel Management Engine BIOS Extension (MEBx) User Guide.
URL: <https://www.intel.com/content/www/us/en/support/articles/000005779/software.html>
9. Baseboard Management Controller (BMC) Security Best Practices.
URL: <https://www.opencompute.org/wiki/Security>
10. BIOS Disassembly Ninjutsu Uncovered – книга Дармавана Салихана.
URL: <https://www.amazon.com/BIOS-Disassembly-Ninjutsu-Uncovered-Darmawan/dp/1597490679>

OPERATIONAL VALIDATION OF A HARDWARE PLATFORM AUDIT METHODOLOGY FOR TRUSTED BOOT SOLUTIONS

stud. Gaberkorn A.E.

National Research University of Electronic Technology

The protection of personal data (PD) in the Russian Federation is governed by Federal Law No. 152-FZ and Government Resolution No. 1119. For Personal Data Processing Systems (PDPS) classified under security levels 1 and 2, threat modeling must explicitly account for risks associated with undeclared hardware and software functionalities. These requirements are further detailed in FSTEC of Russia Order No. 21. Particular emphasis is placed on the system initialization phase, where the absence of covert code modification pathways at the BIOS/UEFI level is critical.

Trusted Boot mechanisms verify the integrity of hardware and software components, employ cryptographic verification, and restrict booting from unauthorized external media. However, the security posture of these mechanisms fundamentally depends on the trustworthiness of the underlying hardware platform. Key threats include unauthorized access via firmware vulnerabilities in components capable of initiating firmware updates or reflashing operations, such as central processing units (CPUs), Baseboard Management Controllers (BMCs), and network interface controllers (NICs). The objective of this study is to conduct an operational validation of a hardware platform audit methodology to assess its suitability for deployment within cryptographic protection systems (CPS).



МЕТОДИКА АВТОМАТИЗИРОВАННОГО ИЗМЕРЕНИЯ РЕАЛЬНЫХ ЗАТУХАНИЙ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ ПРИ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

студ. Яшин В.А.

Национальный исследовательский университет «МИЭТ»

В статье предложена методика автоматизированного измерения реальных затуханий побочных электромагнитных излучений при аттестации объектов информатизации. Представлен разработанный программно-технический комплекс, реализованный в среде LabVIEW и предназначенный для автоматизации управления измерительным оборудованием и регистрации результатов измерений. Для обеспечения удалённого взаимодействия с приборами применяется USB-сервер с поддержкой технологии USB over IP, что позволяет гибко размещать измерительную аппаратуру в условиях проведения испытаний. Использование протокола SCPI обеспечивает совместимость комплекса с широким спектром измерительных приборов и устраняет ограничения, характерные для решений, ориентированных на оборудование конкретных производителей. Описана методика проведения измерений реального затухания ПЭМИ и приведены особенности её практической реализации. Показано, что применение разработанного комплекса позволяет сократить трудоёмкость измерений, снизить влияние человеческого фактора и повысить эффективность проведения многократных измерений в одном направлении.

Одним из наиболее опасных технических каналов утечки информации из объектов информатизации (ОИ) является канал побочных электромагнитных излучений (ПЭМИ), возникающих при работе средств вычислительной техники [1]. Перехват ПЭМИ может осуществляться средствами радиоразведки без физического доступа к оборудованию, что делает данный канал критически значимым с точки зрения обеспечения информационной безопасности.

Для оценки защищённости объекта информатизации проводятся измерения реального затухания ПЭМИ, характеризующего степень ослабления информативного сигнала на пути его распространения от источника до границы контролируемой зоны [2]. Данная процедура является обязательным этапом аттестации на соответствие требованиям информационной безопасности, поскольку позволяет экспериментально подтвердить выполнение условия недопустимости утечки информации по каналу ПЭМИ.

Особую значимость проведение измерений приобретает в случае, когда расчётная зона возможного перехвата информативного сигнала R_2 превышает границу контролируемой зоны $R_{кз}$ (то есть, когда $R_2 > R_{кз}$). В указанной ситуации существует потенциальная возможность распространения информативного сигнала за пределы контролируемой территории, что не позволяет ограничиться расчётной оценкой и требует обязательной экспериментальной проверки фактического уровня затухания. При этом реальные условия распространения электромагнитных волн, включая влияние отражений, экранирования и дифракции на конструктивных элементах здания и объектах окружающей среды, могут как увеличивать, так и уменьшать дальность распространения сигнала по сравнению с расчётной моделью. В связи с этим измерение реального затухания ПЭМИ выступает необходимым инструментом выявления наиболее опасных направлений утечки информации и количественной оценки эффективности реализованных мер защиты.

Традиционная методика выполнения таких измерений предполагает ручное управление генератором сигналов и анализатором спектра, требует участия двух операторов и значительных временных затрат на обработку каждой частотной точки. Это обуславливает высокую трудоёмкость процесса и повышает вероятность возникновения ошибок, связанных с влиянием человеческого фактора. На рынке представлены отдельные автоматизированные решения, например, комплексы «Стентор» (ООО ЦБИ «МАСКОМ») и «Зонд» (АО «НЕЛК»), которые, как правило, жёстко привязаны к конкретным моделям измерительного оборудования. Это требует приобретения дорогостоящих приборов определённых производителей и ограничивает гибкость применения. Разработанный программно-технический комплекс лишён указанных недостатков, поскольку поддерживает любые измерительные приборы, реализующие управление по протоколу SCPI [3]. Это обеспечивает универсальность решения и возможность использования уже имеющегося оборудования без дополнительных затрат.

Для проведения измерений необходим лабораторный испытательный стенд (рисунок 1), обеспечивающий автоматизированное управление измерительным оборудованием и регистрацию результатов.

В состав стенда входят: управляющий ноутбук с разработанным программным обеспечением в среде LabVIEW, генератор сигналов НОВО ГСП-10 (с поддержкой протокола SCPI), портативный анализатор спектра R&S FSH8, излучающая широкополосная антенна от компании НОВО АШП-03, а также приёмная измерительная антенна НБА-02 с диапазоном рабочих частот от 0,009 до 2500 МГц.

Для организации удалённого управления измерительным оборудованием используется USB-сервер DN-USB4-V4, обеспечивающий передачу данных по сети Wi-Fi [4]. Генератор сигналов НОВО ГСП-10 подключается к управляющему ноутбуку через USB-интерфейс с использованием USB-сервера, что

обеспечивает удалённый доступ к прибору по сети и возможность управления им с помощью команд SCPI. Такое решение позволяет гибко размещать измерительное оборудование независимо от условий проведения измерений на объекте информатизации.

Анализатор спектра R&S FSH8 подключается к управляющему ноутбуку напрямую по интерфейсу LAN и используется для регистрации уровней сигналов в заданных точках измерений.

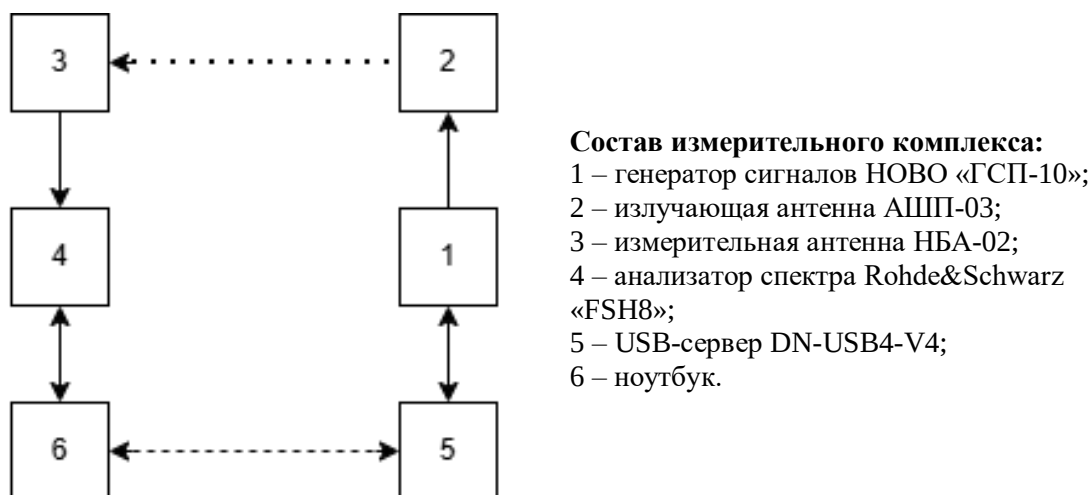


Рисунок 1 – Структурно-функциональная схема автоматизированной системы измерения реальных затуханий ПЭМИ

Измерения реального затухания ПЭМИ выполняются в направлении ближайших мест возможного размещения технических средств разведки (стационарных, мобильных и переносных), расположенных за пределами контролируемой зоны. Схема взаимного расположения элементов измерительного комплекса при проведении измерений представлена на рисунке 2.

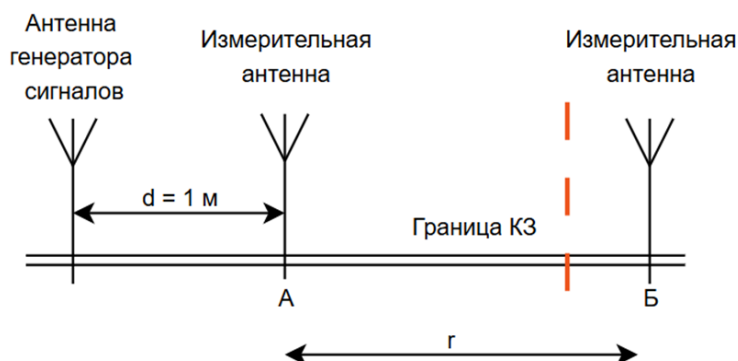


Рисунок 2 – Схема измерения реального затухания ПЭМИ на трассе СВТ – ТСР

Методика проведения измерений включает следующие этапы.

1. Генератор сигналов НОВО «ГСП-10» подключается к излучающей антенне АШП-03, которая устанавливается в месте расположения средства вычислительной техники.
2. На расстоянии 1 м от излучающей антенны устанавливается измерительная активная широкополосная антенна НБА-02 (точка А), которая подключается к анализатору спектра R&S FSH8, расположенного на расстоянии 3 м от всей системы.
3. Генератор сигналов подключается к управляющему ноутбуку через USB-интерфейс с использованием USB-сервера DN-USB4-V4 по технологии USB over IP. Анализатор спектра подключается к управляющему ноутбуку по интерфейсу LAN.
4. Для управления анализатором спектра необходимо создать изолированную локальную подсеть. Управляющему ноутбуку присваивается статический IP-адрес, например, 192.168.1.10, а анализатору спектра — 192.168.1.11. Для управления генератором сигналов, работающего через USB-сервер, на управляющем ноутбуке создаётся виртуальный USB-путём перенаправления сетевого порта (USB over IP).
5. После выполнения всех настроек запускается разработанное программное обеспечение. В процессе работы интерфейс программы в режиме реального времени отображает текущее состояние подключения

измерительных приборов, а также их текущие параметры. При необходимости указанные параметры могут быть изменены непосредственно через программное обеспечение.

6. В программном обеспечении задаются следующие параметры измерительного цикла: частотная сетка, по которой будут проводиться измерения; максимальный уровень выходной мощности генератора; параметры анализатора спектра (полоса пропускания RBW, полоса обзора SPAN, тип детектора и режим измерений). Ключевым преимуществом разработанного программного обеспечения является возможность задания временной задержки перед началом каждого измерительного цикла. Значение данной задержки определяется временем развёртки (sweep) анализатора спектра и не должно быть менее 300 мс. Указанное ограничение обусловлено необходимостью передачи управляющих команд измерительным приборам по каналу связи, а также временем стабилизации условий приёма сигнала измерительной аппаратурой. При использовании режима усреднения, с целью обеспечения достоверности результатов измерений, рекомендуется выполнять не менее 10 развёрток (sweep).

7. Между антеннами обеспечивается взаимная ориентация, соответствующая максимуму принимаемого сигнала. После завершения настройки параметров проводятся измерения уровня сигнала U_{Ai} , дБ(мкВ) в соответствии с заданной частотной сеткой и установленными параметрами анализатора спектра.

8. Приёмная антенна совместно с анализатором спектра переносится на границу контролируемой зоны (точка В), где необходимо провести дальнейшие измерения. На границе контролируемой зоны, с теми же настройками оборудования и регистрацией уровней сигнала при включённом U_{Bi} , дБ(мкВ) и при выключенном генераторе $U_{Bши}$, дБ(мкВ). При этом излучающая антенна и генератор остаются в исходной точке, а ориентации антенн сохраняются.

9. По завершении измерений полученные результаты сохраняются из ПО в файл формата Excel для последующей обработки, анализа и выполнения расчётов затухания ПЭМИ.

10. Производится расчёт уровней напряжённости электрического поля тестовых сигналов для каждой частоты и каждой контрольной точки:

$$E_{Ai} = U_{Ai} + K_{ai},$$

$$E_{Bi} = 10 * \log(10^{0,1*U_{Bi}} - 10^{0,1*U_{Bши}}) + K_{ai},$$

где E_{Ai} – уровней напряжённости электрического поля тестовых сигналов в точке А на i -й частоте, дБ(мкВ);

E_{Bi} – уровней напряжённости электрического поля тестовых сигналов в точке В на i -й частоте, дБ(мкВ);

K_{ai} – калибровочный коэффициент антенны на i -й частоте, дБ(1/м).

11. Так как дальнейшие расчёты производятся с использованием линейных значений напряжённости поля, полученные уровни переводятся из логарифмической шкалы в амплитудное представление по следующим формулам:

$$E_{Ai}^* = 10^{0,05*E_{Ai}},$$

$$E_{Bi}^* = 10^{0,05*E_{Bi}},$$

где E_{Ai}^* – линейное значение напряжённости электрического поля в точке А на i -й частоте;

E_{Bi}^* – линейное значение напряжённости электрического поля в точке В на i -й частоте.

12. На основе преобразованных значений напряжённостей далее рассчитывается реальное затухание информативного сигнала по каждой i -ой частоте. Для этого используется отношение амплитудных значений:

$$V_r(f_i) = \frac{E_{Ai}^*}{E_{Bi}^*},$$

где $V_r(f_i)$ – значение затухания на частоте f_i .

Значение $V_r(f_i)$ отражает степень ослабления сигнала на пути его распространения от источника до границы КЗ.

Следует учитывать, что в реальных условиях эксплуатации объекта при наличии экранирующих и отражающих преград радиус зоны R_2 может существенно уменьшаться, что дополнительно повышает уровень защищённости от утечки информации по каналу ПЭМИ.

В случае применения средств активной защиты (САЗ) расчёты повторяются с учётом новых параметров шумового сигнала, что позволяет объективно оценить эффективность работы САЗ и степень снижения уровня потенциальной угрозы. При этом актуальность разработанного программного обеспечения возрастает, поскольку в одном направлении может потребоваться многократное проведение измерений при применении активных и пассивных средств защиты.

Описанная методика автоматизированного измерения реальных затуханий ПЭМИ позволяет проводить аттестацию объектов информатизации с меньшими временными затратами и снижением влияния человеческого фактора по сравнению с традиционным ручным подходом. Использование универсального протокола SCPI и технологии USB over IP обеспечивает гибкость и масштабируемость комплекса, его независимость от конкретных моделей измерительных приборов. Применение автоматизированного управления оборудованием и возможности задания временной задержки гарантирует стабильность измерений и достоверность получаемых результатов. Предложенная методика рекомендуется для внедрения в практику аттестационных лабораторий и подразделений технической защиты информации, особенно в условиях необходимости многократных повторных измерений.

Литература

1. Хорев А.А. Техническая защита информации: учеб. пособие: В 3-х т. Т. 1: Технические каналы утечки информации. -М.: НПЦ «Аналитика», 2008. – 436 с.
2. Зайцев, В.Е., Мещеряков, А.И., Шелупанов, А.В. Технические средства и методы защиты информации. – М.: Издательство МГТУ, 2013. – 352 с.
3. Яшин В.А. Автоматизированная система измерения затуханий электромагнитных излучений на объектах информатизации // Радиоэлектронные устройства и системы для инфокоммуникационных технологий (REDS-2025) : сборник докладов Всероссийской конференции (с международным участием), 22–23 мая 2025 г. – Москва : РНТОРЭС им. А.С. Попова, 2025. – С. 447–451. – URL: http://www.rntores.ru/REDS/2025-REDS-80_Sbornik_dokladov_konferencii.pdf (дата обращения: 29.04.2026).
4. Технический паспорт USB-сервера DN-USB4-V4 [Электронный ресурс]. – Режим доступа: <https://server19.ru/files/%D0%9F%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82%20DN-USB.pdf> (дата обращения: 29.04.2026).

THE METHODOLOGY OF AUTOMATED MEASUREMENT OF REAL ATTENUATION OF ELECTROMAGNETIC SIDE EFFECTS DURING CERTIFICATION OF INFORMATIZATION FACILITIES

stud. Yashin V.A.

National Research University of Electronic Technology

The article proposes a method for automated measurement of real attenuation of electromagnetic side effects during certification of informatization facilities. The developed software and hardware package, implemented in the LabVIEW environment and designed to automate the control of measuring equipment and registration of measurement results, is presented. To ensure remote interaction with the devices, a USB server with support for USB over IP technology is used, which allows flexible placement of measuring equipment in test conditions. The use of the SCPI protocol ensures compatibility of the complex with a wide range of measuring instruments and eliminates the limitations typical for solutions focused on equipment from specific manufacturers. The method of measuring the real attenuation of the TEM is described and the features of its practical implementation are given. It is shown that the application of the developed complex makes it possible to reduce the complexity of measurements, reduce the influence of the human factor and increase the efficiency of multiple measurements in one direction.



ИССЛЕДОВАНИЕ МЕТОДОВ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ В РАСПРЕДЕЛЁННЫХ СИСТЕМАХ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

доц. Бутакова Н.Г., студ. Юрченков В.О.

Национальный исследовательский университет «МИЭТ»

В статье рассматривается проблема обеспечения целостности данных в распределённых системах управления базами данных при выполнении распределённых транзакций. Проведен анализ основных угроз нарушения целостности данных, включая рассогласование реплик, частичные отказы узлов, сетевые сбои, задержки передачи сообщений и возможные злонамеренные воздействия со стороны участников системы. Рассмотрены классические механизмы координации распределённых транзакций, такие как протокол двухфазной фиксации транзакций (2PC) и механизм Saga, а также выявлены их ограничения при функционировании в условиях недоверенной среды. Показано, что традиционные механизмы обеспечения согласованности ориентированы на координацию состояния транзакций и не предусматривают встроенных средств криптографического контроля целостности данных, что может приводить к дополнительным рискам нарушения корректности информации.

В статье исследуется применение криптографических методов контроля целостности, основанных на использовании хеш-функций и структур данных типа Merkle-деревьев, которые позволяют формировать уникальные контрольные значения и эффективно выявлять любые изменения данных. Показано, что интеграция криптографических подходов позволяет повысить устойчивость системы к ошибкам синхронизации, сетевым сбоям и злонамеренным воздействиям, а также создавать основу для разработки более надёжных и масштабируемых моделей обеспечения целостности данных в распределённых информационных системах.

Современные информационные системы всё чаще строятся на основе распределённых архитектур. Использование распределённых систем управления базами данных позволяет обеспечить масштабируемость, отказоустойчивость и высокую производительность обработки данных. В таких системах данные могут храниться и обрабатываться на нескольких узлах, взаимодействующих между собой через компьютерную сеть. Одной из ключевых задач функционирования распределённых СУБД является обеспечение целостности и согласованности данных при выполнении распределённых транзакций. В отличие от централизованных систем, в распределённых базах данных изменения могут выполняться одновременно на нескольких узлах системы, что существенно усложняет процессы координации операций и контроля корректности состояния данных.

В распределённых системах существует ряд факторов, способных привести к нарушению целостности данных. Одной из распространённых проблем является рассогласование реплик. В системах с репликацией данные хранятся на нескольких узлах одновременно, и при возникновении сетевых задержек или временных отказов отдельных узлов возможно возникновение ситуаций, при которых различные узлы системы содержат различное состояние данных. Другой важной проблемой являются частичные отказы узлов распределённой системы. В процессе выполнения распределённой транзакции один из узлов может стать недоступным, что приводит к неопределённому состоянию транзакции и необходимости выполнения дополнительных процедур восстановления. Кроме того, в распределённых системах возможны сетевые сбои и задержки передачи сообщений между узлами, которые могут приводить к потере сообщений, повторной отправке операций или нарушению порядка выполнения транзакций. Отдельную категорию угроз составляют злонамеренные воздействия. В условиях недоверенной среды отдельные узлы системы могут передавать искажённые данные, подменять сообщения транзакций или модифицировать журналы операций, что может привести к некорректному состоянию данных.

Для координации выполнения распределённых транзакций применяются специальные протоколы согласования. Одним из наиболее распространённых механизмов является протокол двухфазной фиксации транзакций (Two-Phase Commit, 2PC). Данный протокол предполагает наличие координатора транзакции и набора участников (рисунок 1). На первой фазе координатор отправляет участникам запрос на подготовку транзакции (prepare), в ответ на который каждый узел выполняет локальную проверку возможности фиксации изменений и переходит в состояние ожидания. Участники фиксируют промежуточное состояние (например, записывают данные в журнал), но не завершают транзакцию окончательно.

После получения подтверждений от всех участников координатор принимает глобальное решение о фиксации транзакции и инициирует вторую фазу – отправку команды commit. В случае, если хотя бы один участник не может подготовить транзакцию, координатор инициирует откат (rollback) для всех узлов. Таким образом обеспечивается атомарность выполнения: либо изменения фиксируются на всех узлах, либо не фиксируются ни на одном.

Несмотря на формальную строгость и широкое применение, протокол 2PC обладает рядом существенных недостатков. Одной из ключевых проблем является его блокирующий характер. В случае отказа координатора после завершения фазы подготовки участники оказываются в неопределённом состоянии и

вынуждены ожидать восстановления координатора для получения окончательного решения. Это приводит к блокировке ресурсов и снижению доступности системы.

Кроме того, протокол чувствителен к сетевым задержкам и увеличивает время выполнения транзакций за счёт необходимости обмена несколькими сообщениями между всеми участниками. При увеличении числа узлов накладные расходы возрастают, что негативно влияет на масштабируемость системы. Также следует отметить, что 2PC предполагает корректное поведение всех участников и не защищает от сценариев, связанных с передачей искажённых или подменённых сообщений, что ограничивает его применение в недоверенных распределённых средах.

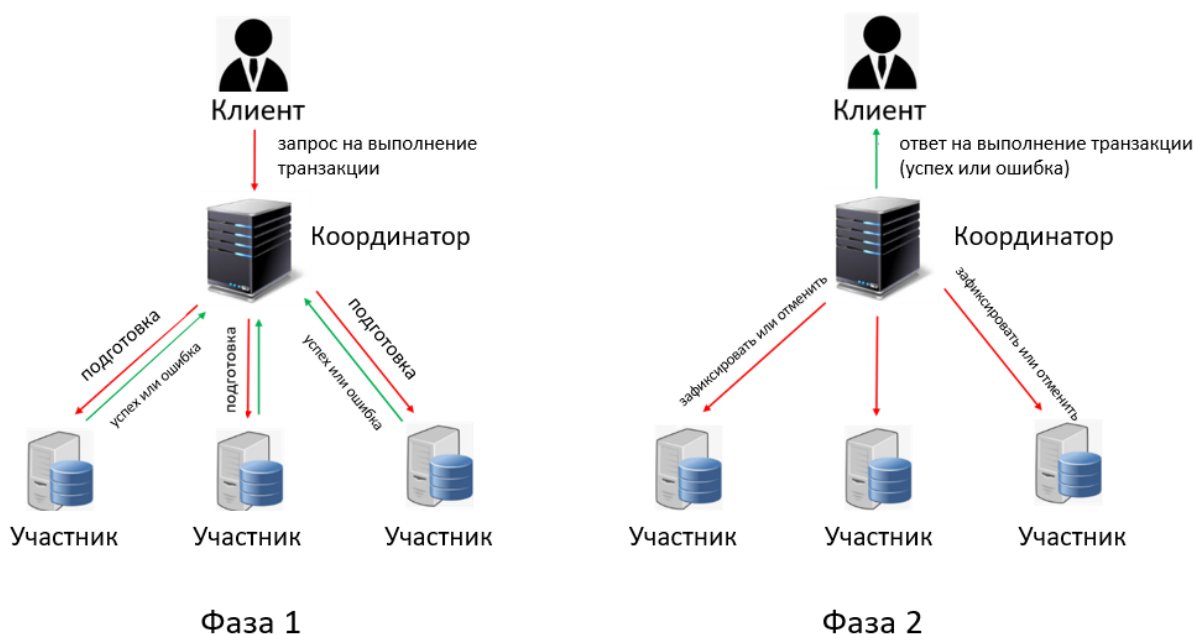


Рисунок 1 – Протокол 2PC

Альтернативным подходом является использование механизма Saga. В данной модели распределённая транзакция разбивается на последовательность локальных транзакций, каждая из которых выполняется независимо на соответствующем узле и может быть компенсирована специальной операцией в случае возникновения ошибки. В отличие от протокола 2PC, Saga не требует глобальной блокировки ресурсов, так как каждая операция фиксируется сразу после выполнения, что позволяет повысить доступность и масштабируемость системы.

Существует два основных способа реализации механизма Saga: оркестрация и хореография. В случае оркестрации управление последовательностью выполнения операций осуществляется центральным компонентом – оркестратором, который определяет порядок вызова локальных транзакций и инициирует компенсационные действия при возникновении ошибок. В модели хореографии отсутствует единый управляющий центр: узлы взаимодействуют друг с другом посредством событий, самостоятельно принимая решения о запуске последующих операций.

При возникновении сбоя на одном из этапов Saga выполняется последовательность компенсирующих транзакций, направленных на отмену уже выполненных операций. Например, если в процессе обработки заказа выполнены операции списания средств и резервирования товара, но произошёл сбой на этапе доставки, система должна выполнить обратные действия – вернуть средства и снять резерв.

Несмотря на преимущества, механизм Saga имеет ряд ограничений. Прежде всего, он не обеспечивает строгую атомарность выполнения операций, поскольку в промежутке между выполнением локальных транзакций система может находиться в частично согласованном состоянии. Кроме того, разработка корректных компенсационных операций является сложной задачей, особенно в системах с большим количеством взаимосвязанных сервисов. Ошибки в реализации компенсаций могут приводить к накоплению неконсистентных данных.

Несмотря на широкое применение протоколов 2PC и Saga, они имеют ряд ограничений с точки зрения обеспечения целостности данных. Основным недостатком является то, что данные механизмы ориентированы прежде всего на согласование состояния транзакций, а не на проверку корректности самих данных. Традиционные протоколы предполагают корректное поведение участников системы и не

предусматривают встроенных средств защиты от злонамеренных воздействий. В частности, они не позволяют обнаружить подмену сообщений между узлами системы или изменение данных после их фиксации. В условиях распределённых систем, функционирующих в недоверенной среде, такие ограничения могут приводить к дополнительным рискам нарушения целостности данных.

В связи с этим актуальной задачей является разработка дополнительных методов контроля целостности данных, способных функционировать в условиях потенциально недоверенной распределённой среды. Одним из перспективных направлений повышения уровня защищённости распределённых систем является использование криптографических методов контроля целостности информации. Основу таких методов составляют криптографические хеш-функции, позволяющие формировать уникальные значения фиксированной длины для произвольных входных данных. Формально хеш-функция может быть представлена следующим образом:

$$h = H(x), \quad (1)$$

где x – исходные данные, H – криптографическая хеш-функция, h – результирующее хеш-значение.

Ключевым свойством хеш-функций является высокая чувствительность к изменению входных данных. Даже незначительное изменение исходного сообщения приводит к существенному изменению результирующего значения:

$$H(x) \neq H(x'), \text{ если } x \neq x' \quad (2)$$

Данное свойство позволяет использовать хеш-функции для выявления любых модификаций данных, возникающих как вследствие ошибок синхронизации, так и в результате злонамеренных воздействий.

Для эффективного контроля целостности больших объёмов информации в распределённых системах применяются структуры данных, основанные на хешировании, в частности Merkle-деревья (рисунок 2). В таких структурах каждому элементу данных сопоставляется хеш-значение, после чего хеши объединяются попарно с формированием значений более высокого уровня. Например, для двух элементов x_1 и x_2 вычисляется:

$$h_{12} = H(H(x_1) || H(x_2)), \quad (3)$$

Рекурсивное применение данного подхода позволяет сформировать корневое хеш-значение:

$$h_{root} = H(h_{12} || h_{34}), \quad (4)$$

которое однозначно характеризует состояние всего набора данных. Изменение любого элемента приводит к изменению соответствующих промежуточных хеш-значений и, в конечном итоге, корневого значения, что позволяет эффективно обнаруживать нарушения целостности.

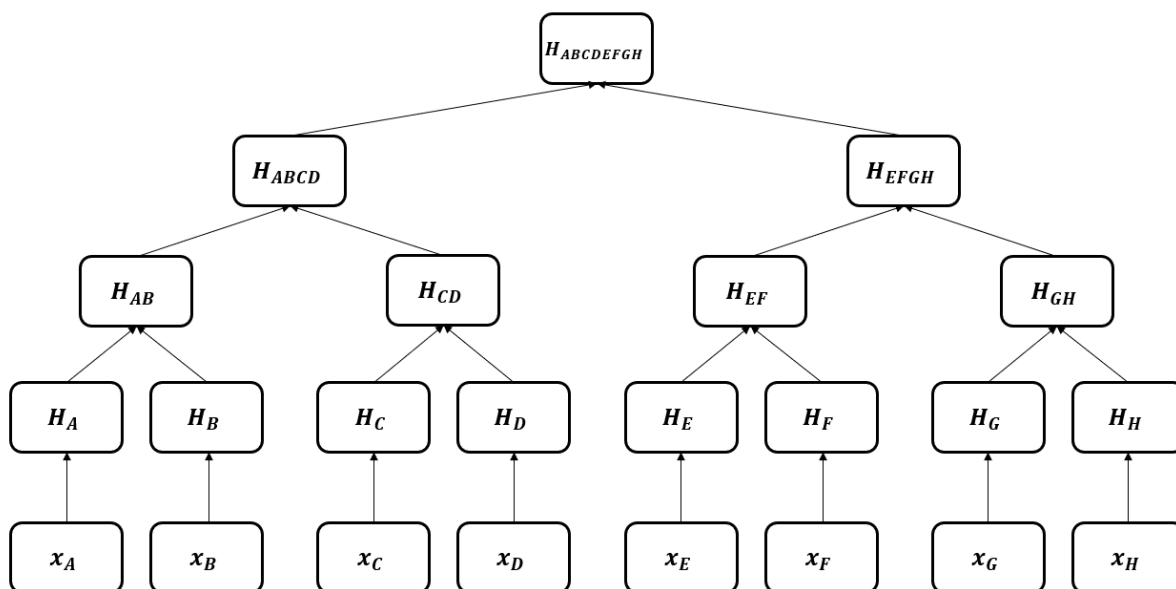


Рисунок 2 – Дерево Меркла

Дополнительным преимуществом применения криптографических методов является возможность их использования в распределённых системах с различным уровнем доверия между участниками. В отличие от традиционных механизмов, основанных на предположении корректного поведения узлов, криптографические подходы позволяют обеспечить верифицируемость данных независимо от источника их получения. Это особенно важно для систем, функционирующих в условиях межорганизационного взаимодействия или облачной инфраструктуры, где отсутствует единый центр доверия.

Следует отметить, что применение хеш-функций и структур типа Merkle-деревьев позволяет не только обнаруживать факт нарушения целостности, но и локализовать область изменения данных. За счёт иерархической организации хеш-значений возможно определить конкретный фрагмент данных, подвергшийся модификации, без необходимости повторной проверки всего набора информации. Это существенно снижает вычислительные затраты и повышает эффективность контроля в системах с большим объёмом данных.

Практическое применение Merkle-деревьев в распределённых СУБД связано, прежде всего, с задачами синхронизации реплик и проверки согласованности данных. Каждый узел системы может формировать корневое хеш-значение, отражающее текущее состояние локальной базы данных. Сравнение корневых хеш-значений между узлами позволяет быстро определить наличие расхождений без передачи полного объёма данных. В случае обнаружения несоответствий выполняется поэтапное сравнение промежуточных хеш-значений, что позволяет локализовать изменённые участки и минимизировать сетевой трафик.

Кроме того, структуры на основе Merkle-деревьев могут применяться при организации журналов транзакций. В этом случае записи журнала объединяются с использованием хеширования, формируя иерархическую или цепочечную структуру, в которой каждая операция связана с предыдущими. Такой подход обеспечивает неизменяемость истории транзакций и позволяет выявлять попытки её модификации. В сочетании с традиционными протоколами согласования это позволяет реализовать дополнительный уровень контроля корректности выполнения распределённых операций.

Таким образом, интеграция криптографических методов контроля целостности данных в распределённые СУБД позволяет значительно повысить уровень защищённости системы и обеспечить дополнительные гарантии корректности обрабатываемой информации. Использование подобных механизмов повышает устойчивость распределённых систем к ошибкам синхронизации, сетевым сбоям и злонамеренным воздействиям, а также создаёт основу для разработки более совершенных моделей обеспечения целостности данных в распределённых системах управления базами данных.

Литература

1. Мельников М.О., Консенсус-алгоритмы в блокчейн-системах // Современные методы прикладной математики, теории управления и компьютерных технологий (ПМТУКТ-2023). – С. 56–58.
2. Канатьев К.Н., Большаков В.Н., Анисимов А.Р., Скоморохина Е.Р., Чикенев С.Д. Анализ возможностей технологии блокчейн в управлении данными // Инновации и инвестиции. – 2023. – №5. – С. 174–178.
3. Емельянов В.Д., Хахина А.М. Особенности проектирования систем распределенного вычисления // Современная школа России. Вопросы модернизации. – 2022. – № 4–1(41). – С. 26–29.

RESEARCH OF METHODS FOR ENSURING DATA INTEGRITY IN DISTRIBUTED DATABASE MANAGEMENT SYSTEMS

assoc. prof. Butakova N.G., stud. Yurchenkov V.O.

National Research University of Electronic Technology

The article addresses the problem of ensuring data integrity in distributed database management systems during the execution of distributed transactions. An analysis of the main threats to data integrity is conducted, including replica inconsistencies, partial node failures, network disruptions, message transmission delays, and potential malicious actions by system participants. Classical mechanisms for coordinating distributed transactions, such as the two-phase commit protocol (2PC) and the Saga pattern, are examined, and their limitations in untrusted environments are identified. It is shown that traditional consistency mechanisms focus on coordinating transaction states and do not provide built-in means for cryptographic data integrity control, which may lead to additional risks of incorrect information.

The article explores the application of cryptographic methods for integrity verification based on hash functions and data structures like Merkle trees, which allow the generation of unique control values and effective detection of any data modifications. It is demonstrated that integrating cryptographic approaches enhances system resilience to synchronization errors, network failures, and malicious actions, and provides a foundation for developing more reliable and scalable models for ensuring data integrity in distributed information systems.



МОДЕЛЬ ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ ТЕХНОЛОГИЧЕСКОЙ СЕТИ АСУ ТП С УЧЕТОМ ОСОБЕННОСТЕЙ ПРОМЫШЛЕННОГО ТРАФИКА И ПРИМЕНЕНИЯ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

студ. Дасибинба У.

Национальный исследовательский университет «МТЭТ»

В статье рассматривается модель обеспечения защищенности технологической сети автоматизированных систем управления технологическими процессами с учетом специфики промышленного трафика и особенностей функционирования производственной инфраструктуры. Проведен анализ характерных угроз и уязвимостей технологических сетей. На основе этого предложена модель защиты, предусматривающая сегментацию сети, применение промышленного межсетевого экранирования и учет контекстных характеристик трафика. Предложенный подход позволяет повысить уровень защищенности технологической сети без нарушения требований к надежности и непрерывности производственных процессов.

Ключевые слова. АСУ ТП, информационная безопасность, технологическая сеть, промышленный трафик, межсетевой экран, сегментация сети.

В условиях стремительной цифровизации промышленности и интеграции производственных систем в единую информационную среду вопросы обеспечения защищенности технологических сетей автоматизированных систем управления технологическими процессами (далее – АСУ ТП) приобретают особую значимость. По данным аналитических исследований, в 2025 году порядка 76% критических кибератак были ориентированы не на извлечение данных, а на разрушение или выведение из строя IT-инфраструктуры организаций [1]. По результату анализа статистики угроз установлено, что в третьем квартале 2025 года доля компьютеров АСУ ТП, на которых были выявлены и заблокированы вредоносные объекты, составила 20,1%, что на 0,4 процентного пункта ниже по сравнению с предыдущим кварталом и является минимальным значением за рассматриваемый период [2]. Динамика данного показателя представлена на рисунке 1.

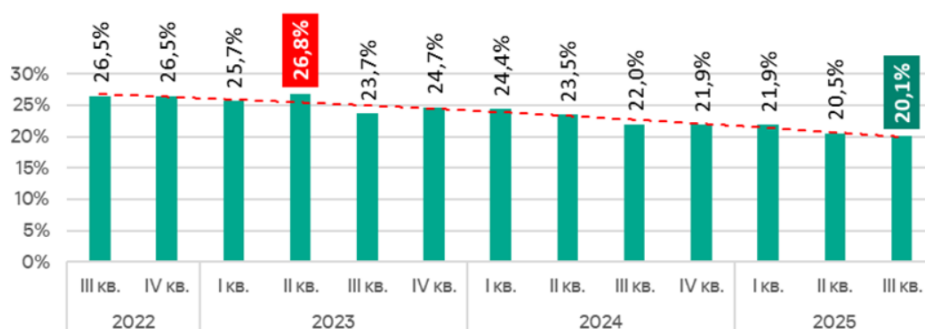


Рисунок 1 – Доля компьютеров АСУ, на которых были заблокированы вредоносные объекты

Несмотря на некоторое снижение данного показателя, уровень угроз для технологических сетей остается значительным, что обусловлено как высокой критичностью объектов управления, так и спецификой промышленного трафика, включающего использование специализированных протоколов, жесткие требования к задержкам и непрерывности функционирования процессов. В этих условиях традиционные подходы к обеспечению информационной безопасности оказываются недостаточно эффективными и требуют адаптации с учетом особенностей АСУ ТП. На основе вышеизложенного следует, что актуальной задачей является разработка модели обеспечения защищенности технологической сети АСУ ТП, учитывающей специфику промышленного трафика и предусматривающей применение специализированных средств защиты, в частности промышленного межсетевого экранирования (далее – МЭ). Реализация подобной модели позволит повысить устойчивость технологической инфраструктуры к современным киберугрозам без нарушения требований к надежности и непрерывности производственных процессов.

На начальном этапе исследования следует определить актуальный перечень угроз, характерных для технологических сетей АСУ ТП, с учетом их архитектурных и функциональных особенностей. Подобный подход позволяет не ограничиваться формальным перечислением типовых рисков, а сформировать целостное представление о направлениях возможного воздействия на элементы системы управления. По результату анализа практики эксплуатации промышленных объектов и рассмотрения современных инцидентов установлено, что угрозы в данном сегменте имеют выраженную специфику, связанную с сочетанием киберфизических процессов, ограничений по обновлению оборудования и высокой зависимостью от непрерывности функционирования.

Существенным отличием технологических сетей является использование специализированных промышленных протоколов (Modbus, OPC, DNP3 и др.), которые изначально не предусматривали встроенных механизмов защиты. Это создает предпосылки для реализации атак, направленных на перехват, подмену или модификацию управляющих команд. Наряду с этим, высокая степень связанности компонентов системы обуславливает каскадный характер последствий, при котором компрометация одного узла может повлечь за собой нарушение работы всей технологической цепочки.

Отдельное внимание следует уделить внутренним угрозам и ошибкам персонала. Совокупность наблюдаемых инцидентов позволяет установить, что значительная часть нарушений связана не с внешним воздействием, а с некорректной эксплуатацией систем, нарушением регламентов доступа и отсутствием контроля действий пользователей. В условиях АСУ ТП подобные факторы приобретают критическое значение, поскольку даже незначительное отклонение параметров может привести к аварийным ситуациям. Обобщение рассмотренных факторов и систематизация угроз, характерных для технологических сетей, представлены в таблице 1

Таблица 1.

Актуальные угрозы технологической сети АСУ ТП и их характеристика

Код угрозы	Наименование угрозы	Описание механизма реализации	Потенциальные последствия для АСУ ТП
У1	Несанкционированный доступ к технологической сети	Получение доступа к сегментам АСУ ТП через уязвимые удаленные интерфейсы, учетные записи или сетевые сервисы	Нарушение конфиденциальности данных, изменение параметров управления, несанкционированное вмешательство в технологический процесс
У1.1	Компрометация учетных данных	Использование слабых паролей, фишинговых атак или утечек для получения доступа к системам управления	Захват контроля над элементами АСУ ТП, выполнение вредоносных команд от имени легитимных пользователей
У2	Внедрение вредоносного программного обеспечения	Проникновение вредоносного кода через внешние носители, сетевые каналы или обновления ПО	Нарушение работы оборудования, скрытое изменение логики управления, блокировка систем
У2.1	Программы-вымогатели	Шифрование данных и инфраструктуры с целью выкупа	Остановка производственных процессов, финансовые потери, невозможность оперативного восстановления
У3	Перехват и модификация промышленного трафика	Использование уязвимостей протоколов для анализа и подмены управляющих команд	Искажение технологических параметров, нарушение корректности работы оборудования
У4	Отказ в обслуживании (DoS/DDoS)	Перегрузка сетевой инфраструктуры или отдельных узлов	Снижение доступности систем, задержки в передаче данных, остановка процессов управления
У5	Внутренние угрозы (инсайдеры)	Умышленные или случайные действия сотрудников	Нарушение регламентов, утечка информации, изменение конфигураций систем
У6	Ошибки конфигурации и администрирования	Неправильная настройка сетевых устройств и средств защиты	Открытые уязвимости, упрощение реализации атак, снижение общего уровня защищенности
У7	Эксплуатация уязвимостей оборудования и ПО	Использование известных и нулевых уязвимостей в компонентах АСУ ТП	Нарушение функционирования систем, получение контроля над устройствами
У8	Нарушение сегментации сети	Отсутствие или некорректная реализация зон безопасности	Распространение атак между сегментами, компрометация критических узлов

По результату анализа представленной классификации можно отметить, что наибольшую опасность представляют комбинированные сценарии угроз, при которых реализуется последовательное воздействие на различные элементы системы. Например, компрометация учетных данных может использоваться как начальный этап для дальнейшего внедрения вредоносного кода или изменения конфигурации оборудования.

Совокупность вышеизложенных результатов позволяет установить, что эффективная защита технологической сети АСУ ТП невозможна без комплексного учета выявленных угроз и их взаимосвязей. Это определяет необходимость разработки модели обеспечения защищенности, ориентированной на предотвращение, обнаружение и локализацию инцидентов с учетом специфики промышленной среды и особенностей сетевого взаимодействия.

На основе проведенного анализа актуальных угроз и особенностей функционирования технологических сетей АСУ ТП представляется целесообразным перейти к формированию комплексной модели обеспечения защищенности. Логика дальнейшего исследования строится не на изолированном применении отдельных средств защиты, а на их согласованном использовании с учетом специфики промышленной среды, требований к надежности и ограничений по задержкам передачи данных. По результату анализа установлено, что наибольшую эффективность демонстрируют решения, ориентированные на структурирование сетевого взаимодействия и контроль трафика на уровне его содержания. В рамках настоящего исследования предлагается модель защиты технологической сети АСУ ТП, предусматривающая сегментацию сети, применение промышленного межсетевого экранирования и учет контекстных характеристик трафика. Ключевая идея модели заключается в разграничении сетевого пространства на функциональные зоны с последующим контролем взаимодействия между ними на основе правил, учитывающих как сетевые параметры, так и особенности технологических протоколов. Общая структура предлагаемой модели представлена на рисунке 2.

Содержательно модель может быть представлена как последовательность уровней защиты, каждый из которых выполняет свою функцию. На нижнем уровне осуществляется локализация оборудования и ограничение прямого доступа к полевым устройствам. На среднем уровне реализуется контроль взаимодействия между контроллерами и системами управления с использованием межсетевого экранирования. На верхнем уровне обеспечивается разграничение доступа между технологической и корпоративной сетью, что предотвращает распространение атак из внешней среды. Особое значение в предложенной модели имеет учет контекста промышленного трафика. В отличие от традиционных IT-сетей, где контроль часто ограничивается анализом IP-адресов и портов, в АСУ ТП требуется интерпретация содержимого команд и их соответствия технологическим сценариям. Для более детального раскрытия каждого уровня и реализуемых механизмов защиты их характеристики в таблице 2.



Рисунок 2 – Модель обеспечения защищенности технологической сети АСУ ТП с применением сегментации и промышленного МЭ

Таблица 2

Характеристика уровней модели защиты технологической сети АСУ ТП

Уровень	Основные функции	Особенности защиты
Уровень 0–1	Непосредственное взаимодействие с технологическим процессом	Максимальная изоляция, отсутствие прямого сетевого доступа, физическая и логическая защита
Уровень 2	Управление оборудованием, обработка сигналов	Ограничение доступа, фильтрация команд, контроль промышленных протоколов
Уровень 3	Мониторинг и управление процессами	Применение промышленного межсетевого экрана, анализ трафика на уровне команд
Уровень 3.5	Буфер между технологической и корпоративной сетью	Двойное межсетевое экранирование, контроль обмена данными, изоляция сервисов
Уровень 4	Бизнес-процессы, ERP, рабочие станции	Разграничение доступа, классическое межсетевое экранирование, контроль пользователей
Внешний уровень	Внешние взаимодействия	VPN, аутентификация, защита периметра

По результату анализа представленной структуры можно установить, что ключевым элементом модели является не просто наличие межсетевых экранов, а их корректное размещение между уровнями с учетом функционального назначения сегментов. Это обеспечивает поэтапную фильтрацию трафика и исключает неконтролируемое взаимодействие между компонентами системы. Совокупность предложенных решений позволяет говорить о формировании многоуровневой модели защиты, ориентированной на предотвращение распространения угроз, локализацию инцидентов и обеспечение устойчивости технологической сети. На основе вышеизложенного следует, что интеграция сегментации сети и промышленного межсетевого экранирования с механизмами контекстного анализа трафика является обоснованным направлением повышения уровня защищенности АСУ ТП в современных условиях.

В ходе проведенного исследования был выполнен анализ актуальных угроз, характерных для технологических сетей АСУ ТП, с учетом современных тенденций развития кибератак и специфики промышленной среды. Установлено, что основную опасность представляют комбинированные сценарии атак, ориентированные на нарушение функционирования инфраструктуры и технологических процессов. На основе рассмотренных факторов предложена модель обеспечения защищенности технологической сети, базирующаяся на принципах сегментации, межсетевого экранирования и контекстного анализа промышленного трафика. Разработанная модель учитывает архитектурные особенности АСУ ТП и направлена на предотвращение распространения угроз между уровнями системы. Совокупность результатов позволяет сделать вывод о том, что применение многоуровневого подхода с четким разграничением зон и контролем взаимодействия между ними обеспечивает повышение устойчивости технологической сети к современным киберугрозам. На основе вышеизложенного следует, что интеграция промышленного межсетевого экранирования с механизмами анализа трафика является обоснованным и практически применимым направлением развития систем защиты АСУ ТП.

Литература

1. 76% кибератак в 2025 году были направлены на уничтожение инфраструктуры компаний.
Электронный ресурс. Режим доступа: <https://clck.ru/3StaUk> (дата обращения: 01.04.2026 г.).
2. Айдинян А.Р., Кирсанов Д.Г. Обеспечение информационной безопасности в производственной сети промышленного предприятия // Вестник ДГТУ. Технические науки. 2025. №1. С. 39-48.
3. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты // Вопросы кибербезопасности. 2019. №3 (31). С. 63-71.
4. Петрова Л.О., Малышев В.С. Надежность и информационная безопасность автоматизированных систем управления технологическими процессами (АСУ ТП) // Вестник магистратуры. 2024. №3-1 (150). С. 18-20.

5. Бузмаков П. О. Методы защиты автоматизированных систем управления технологическими процессами от кибератак // Вестник магистратуры. 2023. №2-1 (137). С. 4-5.
6. Конев А.А., Репкин В.С., Цимбалов К.И. Сценарий атаки на автоматизированную систему управления технологическим процессом с учетом уязвимости протокола Modbus TCP // Программные продукты и системы. 2024. №4. С. 600-610.
7. Угланова Е.С., Пальчун Е.Н. Технические средства с функцией межсетевого экранирования // Известия ТулГУ. Технические науки. 2024. №4. С. 176-179.

**A MODEL FOR ENSURING THE SECURITY TECHNOLOGICAL
NETWORK AUTOMATED PROCESS CONTROL SYSTEM,
TAKING INTO ACCOUNT THE FEATURES OF INDUSTRIAL
TRAFFIC AND THE USE OF INTER-NETWORK SHIELDING**

student Dasibinba U.

National Research University of Electronic Technology

The article considers a model for ensuring the security of a technological network of automated process control systems, taking into account the specifics of industrial traffic and the functioning of the production infrastructure. The analysis of typical threats and vulnerabilities of technological networks. Based on this, a protection model proposed that includes network segmentation, the use of industrial firewalls, and the consideration of traffic context characteristics. This approach allows for enhancing the security of the technological network without compromising the reliability and continuity of production processes.

Key words. Automated process control system, information security, technological network, industrial traffic, firewall, network segmentation.



РАЗРАБОТКА МЕТОДИКИ ОБНАРУЖЕНИЯ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА МЕТОДАМИ СТАТИСТИЧЕСКОГО АНАЛИЗА В DLP-СИСТЕМАХ

студ. Дмитриев И.А.

Национальный исследовательский университет «МИЭТ»

В работе предложена двухуровневая методика статистической фильтрации сетевого трафика для DLP-систем, основанная на совместном применении энтропии Шеннона и коэффициента Хёрста. Определены пороговые значения для отсева зашифрованного трафика (энтропия $> 7,5$ бит/байт) и выявления структурированных данных (энтропия $< 6,0$ бит/байт). Для потоковой классификации установлены границы коэффициента Хёрста: $H > 0,65$ – персистентность (передача файлов), $H < 0,5$ – антиперсистентность (легитимный веб-сёрфинг). Разработано правило обработки переходной зоны $0,5 \leq H \leq 0,65$ с использованием средней энтропии потока и коэффициента вариации размеров пакетов. Экспериментальные исследования на размеченных датасетах подтвердили статистическую значимость различий ($p < 0,001$ и $p < 0,01$) и показали снижение вычислительной нагрузки на модуль глубокого анализа пакетов (DPI) на 87% при производительности обработки 1 Гбит/с на одном ядре CPU. Полученные результаты демонстрируют возможность применения разработанной методики в корпоративных DLP-системах для повышения эффективности обнаружения утечек в зашифрованных каналах.

Введение

В условиях цифровой трансформации DLP-системы (Data Leak Prevention) стали критическим элементом защиты организаций от утечек конфиденциальной информации. Повсеместное внедрение шифрования сетевого трафика (HTTPS, TLS, VPN) существенно ограничивает возможности классических DLP-решений, построенных на технологии глубокого анализа пакетов (Deep Packet Inspection – DPI). DPI требует расшифровки каждого соединения для поиска сигнатур или регулярных выражений, что технически сложно и юридически ограничено, а также приводит к росту вычислительных затрат при работе на высокоскоростных каналах.

Существующие подходы к решению этой проблемы – проксирование трафика с подстановкой сертификатов или полный отказ от анализа зашифрованных сессий – имеют существенные недостатки: первый нарушает принцип сквозного шифрования (E2EE) и требует доверия к промежуточному узлу, второй оставляет канал утечек открытым.

Альтернативой служат методы статистического анализа, позволяющие оценивать свойства данных без их расшифровки. В частности, энтропия Шеннона отражает равномерность распределения байт в пакете, а коэффициент Хёрста характеризует самоподобие временного ряда пакетов в потоке. Эти метрики могут служить признаками для дифференциации зашифрованного трафика от незашифрованного, а также для выявления потоков, связанных с передачей больших объёмов структурированных данных (текстовые файлы, дампы баз данных, таблицы), которые потенциально содержат конфиденциальную информацию.

В связи с этим разработка методики обнаружения аномалий сетевого трафика на основе статистического анализа является актуальной задачей. В рамках данной работы ставится задача создания двухуровневой методики фильтрации, обеспечивающей: первичный отсев зашифрованного трафика по энтропии Шеннона; потоковую классификацию по коэффициенту Хёрста с обработкой переходной зоны; точечное применение DPI только к подозрительным потокам.

Целью работы является совершенствование архитектуры DLP-систем на основе методов статистического анализа для повышения точности обнаружения инцидентов безопасности и снижения вычислительной нагрузки.

Основная часть

Стандартная DPI-система, основанная на сигнатурах и регулярных выражениях, эффективна при работе с незашифрованными данными, однако при обработке зашифрованного трафика сталкивается с дилеммой: либо пропустить потенциальную утечку, либо организовать расшифровку, что требует значительных ресурсов и часто невозможно юридически. На высокоскоростных каналах (1 Гбит/с и выше) полный DPI всех потоков приводит к потерям пакетов и недопустимым задержкам.

Рассмотрение DLP-системы как интеллектуального фильтра, а не просто инструмента для чтения трафика, меняет парадигму безопасности с тотального контроля на умное управление рисками. DPI применяется точно – только к потокам, которые по статистическим характеристикам напоминают незашифрованные структурированные данные, потенциально содержащие конфиденциальную информацию. Критерием для первичной фильтрации служат статистические метрики, оцениваемые без расшифровки.

Для блока данных (полезной нагрузки пакета) энтропия Шеннона (h) – частота встречаемости байта с конкретным значением в блоке. Максимальное значение (8 бит/байт) достигается при равномерном

распределении байт, что характерно для шифрованных или сжатых данных. Для текстов на естественном языке типичная энтропия составляет 4–5 бит/байт, для структурированных данных (CSV, дампы баз) – 5–6 бит/байт. Вычислительная сложность оценки энтропии – $O(N)$, что при реализации с SIMD-инструкциями (AVX2) позволяет обрабатывать более 10 Гбит/с на одном ядре CPU.

Коэффициент Хёрста (H) характеризует долговременную зависимость (самоподобие) временного ряда. В работе используется R/S-метод анализа. Для шифрованных сессий коэффициент Хёрста близок к 0,5, что указывает на антиперсистентность. Для потоков, связанных с передачей больших объёмов данных (файлы, дампы), характерна персистентность с $H > 0,5$.

Для уточнения классификации в переходных зонах используется коэффициент вариации размеров пакетов $CV = \sigma/\mu$, где σ – стандартное отклонение, μ – средний размер пакета в потоке. Для потоковой передачи больших файлов размер пакетов близок к MTU (≈ 1500 байт), $CV < 0,4$. Для интерактивного трафика (веб, SSH, команды) размеры пакетов варьируются от 64 до 1500 байт, $CV > 0,8$.

На основе выбранных метрик разработана двухуровневая методика, реализованная в прототипе на базе платформы Zeek.

Уровень 1 – пакетная фильтрация по энтропии Шеннона. Для каждого пакета вычисляется энтропия полезной нагрузки. Применяются следующие пороги (установлены эмпирически на основе анализа датасетов CIC-IDS2017 и собственных записей трафика):

$h > 7,5$ бит/байт – шифрование или сжатие (DPI бесполезен без расшифровки), пакет отбрасывается;

$h < 6,0$ бит/байт – нешифрованные структурированные данные, пакет передаётся в скользящее окно для накопления (100 пакетов или 1 МБ);

$6,0 \leq h \leq 7,5$ – переходная зона, пакет также буферизуется для последующего потокового анализа.

Уровень 2 – потоковая классификация по коэффициенту Хёрста. По заполнении скользящего окна вычисляется коэффициент Хёрста:

$H > 0,65$ – персистентность (долговременная зависимость), характерно для передачи больших файлов, дампов БД, поток направляется на DPI для глубокого семантического анализа;

$H < 0,5$ – антиперсистентность (интерактивный веб-сёрфинг, шифрованные сессии без передачи файлов), поток пропускается без DPI;

$0,5 \leq H \leq 0,65$ – переходная зона (слабая персистентность), применяется следующий алгоритм уточнения.

Обработка переходной зоны ($0,5 \leq H \leq 0,65$).

Шаг 1. Вычисление средней энтропии потока $\bar{h}$:

$\bar{h} < 6,0$ – поток нешифрованный, на DPI;

$\bar{h} > 7,0$ – поток шифрованный, пропустить;

$6,0 \leq \bar{h} \leq 7,0$ – перейти к шагу 2.

Шаг 2. Анализ коэффициента вариации размеров пакетов (CV):

$CV > 0,8$ – высокая дисперсия (интерактивный трафик), пропустить;

$CV < 0,4$ – низкая дисперсия (потоковая передача), на DPI;

$0,4 \leq CV \leq 0,8$ – промежуточный случай, решение откладывается (накопить больше пакетов или передать на DPI с низким приоритетом).

Действия при обнаружении соответствующего трафика сведены в таблицу 1.

Таблица 1.

Действия DLP-системы в зависимости от типа трафика и значений выбранных метрик

Тип трафика	Энтропия	Коэф Хёрста	Действие
Шифрованный (HTTPS, TLS)	$< 6,0$	$> 0,65$	направить на DPI
Интерактивный веб-сёрфинг	$> 7,5$	$< 0,5$	пропустить
Переходная зона	$6,0-7,5$	$0,5-0,65$	уточнение по CV

Для обоснования применимости выбранных метрик сформулированы две статистические гипотезы.

Гипотеза H1 (энтропия Шеннона): распределение энтропии пакетов, содержащих конфиденциальную информацию (текст, таблицы), статистически значимо ниже распределения энтропии зашифрованного трафика. Ожидаемые средние: $h_{\text{text}} \approx 4,5$ бит/байт, $h_{\text{cipher}} \approx 7,9$ бит/байт. Проверка: t-критерий Стьюдента для независимых выборок. Ожидаемый p-value $< 0,001$.

Гипотеза H2 (коэффициент Хёрста): распределение коэффициента Хёрста для потоков с передачей файлов статистически значимо выше, чем для интерактивных зашифрованных сессий. Ожидаемые средние: $h_{\text{file}} \approx 0,72$, $h_{\text{web}} \approx 0,5$. Проверка: U-критерий Манна–Уитни. Ожидаемый p-value $< 0,01$.

Для проверки работоспособности разработанной методики создан лабораторный стенд.

Состав стенда:

ПК с CPU Intel i5, 16 ГБ RAM, сетевая карта 2,4 Гбит/с, ОС Ubuntu 24.04.

Платформа Zeek (версия 6.0) с модулями на C, использующими SIMD-инструкции (AVX2).

Датасеты: CIC-IDS2017, собственная запись трафика в локальной сети МИЭТ (текстовые файлы, дампы, HTTPS-сессии).

Тестирование проводилось для трёх сценариев.

Сценарий 1 – передача текстового файла (10 МБ) через HTTP. Средняя энтропия пакетов $\approx 4,8$ бит/байт, коэффициент Хёрста $\approx 0,71$. Результат: поток направлен на DPI (верное обнаружение потенциальной утечки).

Сценарий 2 – легитимная HTTPS-сессия (веб-сёрфинг). Энтропия пакетов $\approx 7,9$ бит/байт (отброшена на уровне 1), коэффициент Хёрста $\approx 0,5$. Результат: поток пропущен (ложных срабатываний нет).

Сценарий 3 – смешанный трафик (решение отложено). Коэффициент Хёрста = 0,58 (переходная зона), средняя энтропия потока = 6,5 бит/байт, CV = 0,52. Результат: решение отложено (накопление дополнительных пакетов) – корректное поведение.

Проверка статистических гипотез на размеченных данных подтвердила значимые различия:

Для H1: $t = 34,2$, $p < 0,001$.

Для H2: $U = 1250$, $p < 0,01$.

Разработанный прототип на базе Zeek с SIMD-инструкциями показал следующие результаты:

Обработка трафика до 1 Гбит/с на одном ядре CPU без потерь пакетов.

Снижение нагрузки на модуль DPI на 87% – DPI применяется только к 13% потоков, прошедших статистическую фильтрацию.

Задержка обработки не превышает 1 мс для уровня 1 и 50 мс для уровня 2 (накопление окна).

Анализ результатов

В результате выполнения работы проведён анализ ограничений классических DLP-систем, основанных на тотальном DPI. Обоснован выбор сигнатурного статистического метода с использованием энтропии Шеннона и коэффициента Хёрста. Разработана двухуровневая методика фильтрации трафика, определены пороговые значения для отсева зашифрованных данных и выявления структурированных потоков. Сформулированы и экспериментально подтверждены статистические гипотезы о различии трафика утечек и легитимного трафика.

К основным преимуществам разработанной методики относятся:

Низкий уровень ложных срабатываний – подтверждён экспериментально (отсутствие ложных срабатываний для HTTPS-сессий).

Модульность архитектуры – возможность интеграции с любым DPI-модулем.

Высокая производительность – обработка 1 Гбит/с на одном ядре CPU благодаря SIMD-ускорению.

Снижение вычислительных затрат – DPI применяется точно, нагрузка снижена на 87%.

Работа без расшифровки – соблюдение юридических и технических ограничений.

В ходе работы также получены следующие результаты:

1. Описаны ограничения DPI-подхода в современных высокоскоростных и зашифрованных сетях, обоснована необходимость предварительной статистической фильтрации трафика.

2. Определены ключевые статистические метрики, пригодные для различения структурированных и неструктурированных данных без расшифровки: энтропия Шеннона, коэффициент Хёрста и коэффициент вариации размеров пакетов для переходных зон.

3. Разработана двухуровневая методика фильтрации с эмпирическими порогами: на уровне пакетов $h > 7,5$ – отбросить, $h < 6,0$ – анализировать далее; на уровне потоков $H > 0,65$ – на DPI, $H < 0,5$ – пропустить; для переходной зоны $0,5 \leq H \leq 0,65$ – уточнение по средней энтропии и CV.

4. Сформулированы и экспериментально подтверждены статистические гипотезы ($p < 0,001$ и $p < 0,01$), доказывающие пригодность выбранных метрик для классификации.

5. Реализован прототип на базе платформы Zeek с высокопроизводительными расчётами на C (SIMD). Экспериментальные исследования показали снижение нагрузки на DPI на 87% при обработке 1 Гбит/с на одном ядре CPU.

Полученные результаты демонстрируют возможность применения разработанной методики в корпоративных DLP-системах для повышения защищённости от утечек конфиденциальной информации через зашифрованные каналы. Дальнейшие исследования будут направлены на внедрение методики в

промышленную DLP-систему, тестирование на реальном трафике крупного предприятия, а также адаптацию метода для обнаружения утечек в протоколах с фиксированным размером пакетов (например, VoIP).

Литература

1. Добряков В.И., Смирнов А.А. Выявление особенностей зашифрованного трафика для различной пользовательской активности в глобальных системах информационного обмена // Вопросы кибербезопасности. 2023. № 2. С. 45–53.
2. Шелухин О.И., Судариков Р.А. Анализ информативных признаков в задачах обнаружения аномалий трафика статистическими методами // Электросвязь. 2022. № 5. С. 32–38.
3. Шелухин О.И., Рыбаков С.Ю., Ванюшина А.В. Оценка характеристик мультифрактального спектра фрактальной размерности сетевого трафика и компьютерных атак в IoT // T-Comm. 2021. Т. 15, № 7. С. 62–69.
4. The Zeek Network Security Monitor [Электронный ресурс]. URL: <https://zeek.org/> (дата обращения: 20.02.2026).
5. ГОСТ Р 58428-2019. Защита информации. Системы предотвращения утечек конфиденциальной информации. Основные положения. – М.: Стандартинформ, 2019.
6. Остапенко А.Г., Иванкин М.П., Савенков Г.А. Обнаружение и нейтрализация вторжений в распределенных информационных системах. – Воронеж: ВГТУ, 2013. – 87 с.

DEVELOPMENT OF A METHOD FOR DETECTING NETWORK TRAFFIC ANOMALIES USING STATISTICAL ANALYSIS METHODS IN DLP SYSTEMS

Stud. Dmitriev I.A.

National Research University of Electronic Technology

This paper proposes a two-level method for statistical filtering of network traffic for DLP systems based on the combined use of Shannon entropy and the Hurst exponent. Thresholds are defined for discarding encrypted traffic (entropy > 7.5 bits/byte) and identifying structured data (entropy < 6.0 bits/byte). For flow classification, Hurst exponent boundaries are established: $H \geq 0.65$ – persistence (file transfer), $H \leq 0.55$ – random process (legitimate web surfing). A rule for processing the transition zone $0.55 < H < 0.65$ using the average flow entropy and the coefficient of variation of packet sizes is developed. Experimental studies on labeled datasets confirmed the statistical significance of the differences ($p < 0.001$ and $p < 0.01$) and showed a 87% reduction in the computational load on the deep packet inspection (DPI) module at a processing rate of 1 Gbit/s on a single CPU core. The obtained results demonstrate the possibility of applying the developed method in corporate DLP systems to improve the efficiency of leak detection in encrypted channels.



АЛГОРИТМ РАБОТЫ ГЕНЕРАТОРА ТЕСТОВЫХ РЕЧЕВЫХ СИГНАЛОВ С РЕГУЛИРУЕМЫМИ ШУМОВЫМИ И СПЕКТРАЛЬНЫМИ СОСТАВЛЯЮЩИМИ

студ. Денисов В.Д., проф. Душкин А.В., студ. Облиенко А.В.

Национальный исследовательский университет «МИЭТ»

В настоящей работе рассматривается алгоритм работы генератора тестовых речевых сигналов с регулируемыми шумовыми и спектральными составляющими. Предлагаемый метод позволяет осуществлять формирование новых аудиоданных, основанных на исходных данных, к которым были применены различные типы искажений с заранее определенными параметрами. Основное внимание уделяется формальному описанию алгоритма, который включает в себя предварительную обработку исходных аудиофайлов, добавление шумовых составляющих с заданными значениями отношения сигнал/шум, формирование тональных помех, применение преобразований нацеленных на изменение спектральных характеристик сигнала, а также одновременное использование выше описанных искажений в различных комбинациях. Применение разработанной модели позволяет получать тестовые аудиофайлы, которые могут быть использованы для проведения последующих исследований в таких областях как цифровая обработка речи, шумоподавление, восстановление речевых сигналов, оценка отношения сигнал/шум, классификация искажений и анализ эффективности работы систем автоматизированного распознавания речи.

Введение.

Аудиофайлы, которые содержат человеческую речь, широко используются в системах автоматизированной обработки речи, голосового управления, телекоммуникаций, аналитики аудиоданных и цифровой обработки сигналов. Однако в реальных условиях сигнал, содержащий речь, зачастую не поступает в целевые системы в чистом, неискаженном виде, так как подвергается воздействию фоновых шумом, аппаратных искажений. Кроме того, свой вклад в искажения вносят также не идеальность среды распространения акустического сигнала и приемных устройств.

Во время проведения исследований алгоритмов, работающих с обработкой речевых сигналов, важную роль играет набор тестовых данных. Для эффективных исследований необходимо иметь возможность работать с данными, параметры искажений которых должны быть не только настраиваемыми, но и повторимыми [1, 2]. Записи с реальными зашумлениями и искажениями не всегда подходят для исследовательских целей в силу того, что параметры искажений, влияющих на полезный сигнал точно не известны. Так же важно отметить что реальные зашумленные записи исключают возможность исследования влияния отдельных параметров на исходные данные и затрудняет анализ вклада каждого из них.

Одним из подходов к решению данной проблемы является создание аудиоданных с заданными параметрами [3, 6], искусственно искаженных определенным алгоритмом. В таком случае из эталонной и неискаженной записи формируется как основа, к которой последовательно применяются различные заранее определенные преобразования. Применение такого подхода позволяет получить множество искаженных сигналов, каждый элемент которого определяется параметрами применяемых искажений. Полученное множество сигналов может быть использовано в дальнейших исследованиях.

Целью данной работы является описание алгоритма работы генератора тестовых речевых аудиосигналов с управляемыми шумовыми и спектральными искажениями. Особое внимание уделяется формализации структуры алгоритма, математической модели формирования искаженных сигналов и способами контроля корректности получаемых данных.

Постановка задачи

Пусть задано множество исходных аудиоданных

$$X = \{x_1[n], x_2[n], \dots, x_m[n]\}, \quad (1)$$

где $x_i[n]$ — дискретный речевой сигнал, m — количество исходных аудиофайлов, n — номер отсчета. Необходимо сгенерировать множество производных сигналов

$$Y = \{y_1[n], y_2[n], \dots, y_m[n]\}, \quad (2)$$

каждый элемент которого получается путем применения одного или нескольких преобразований к исходному сигналу.

Рассмотрим четыре возможных режима формирования выходных данных: добавление в исходные аудиофайлы шумовой составляющей, добавление тональных сигналов, применение спектральных искажений, а также комбинированный вариант, который реализует последовательное применения преобразований различных типов к эталонному аудиофайлу [3-5]. При этом каждый этап преобразований (как одиночных, так и комбинированных) должен быть настраиваемым, что достигается изменением параметров преобразования.

Цель алгоритма заключается в обеспечении воспроизводимого получения множества Y на основе исходного множества X и картежа параметров генерации. Важным моментом является сохранение связи

между множествами X и Y , что позволяет использовать полученные данные в последующем анализе влияния различных параметров на свойства речевых сигналов.

Математическая модель формирования искаженного сигнала

Эталонный речевой сигнал представляется дискретной последовательностью

$$x[n], \quad n = 0, 1, 2, \dots, N - 1, \quad (3)$$

где N — количество отсчетов. Обобщенная модель формирования искаженного сигнала задается выражением

$$y[n] = H\{x[n] + \alpha v[n]\}, \quad (4)$$

где $v[n]$ — шумовая или тональная помеха, α — коэффициент масштабирования помехи, $H\{\}$ — оператор спектрального преобразования, а $y[n]$ — сформированный сигнал.

Данная модель допускает частные случаи. Если необходимо сгенерировать сигнал только с шумовым воздействием, оператор спектральных преобразования $H\{\}$ не применяется и выражение 4 сводится к выражению 5

$$y[n] = x[n] + \alpha v[n]. \quad (5)$$

При необходимости получения выходного сигнала исключительно со спектральными искажениями, то выражение 4 сводится к выражению 6

$$y[n] = H\{x[n]\}. \quad (6)$$

Также алгоритм допускает применение нескольких преобразований одного типа к эталонному сигналу. Если к исходному сигналу применяются несколько спектральных преобразований, например, несколько фильтров, выходной сигнал может быть определен как вложение операторов друг в друга

$$y[n] = H_k\{H_{k-1}\{\dots H_2\{H_1\{x[n]\}\}\dots\}\}, \quad (7)$$

где $H_1, H_2, H_{k-1}, \dots, H_k$ — последовательно применяемые операторы спектральных преобразований, а k — количество преобразований.

В случае применения нескольких шумовых преобразований, формула получения выходного сигнала может быть описана следующим образом

$$y[n] = x[n] + \sum_{i=1}^r \alpha_i v_i[n], \quad (8)$$

где $v_i[n]$ — i -я шумовая или тональная составляющая; α_i — коэффициент масштабирования соответствующей помехи; r — количество добавляемых преобразований. Такой подход позволяет моделировать ситуации, в которых на исходное аудио воздействует шумовой сигнал, причем разницы между шумом и тональным сигналом в контексте вычислений нет.

Для случаев, когда на исходный сигнал воздействует случайное количество как спектральных преобразований, так и шумовых, выражение выходного сигнала можно получить, применив принцип выражения 4 и допустить, что в выражении 7 $x[n]$ равняется $y[n]$ из выражения 8, таким образом, получаем следующее выражение, которое описывает общий случай воздействия случайного количества спектральных преобразований и шумовых воздействий на эталонный сигнал

$$y[n] = H_k\{H_{k-1}\{\dots H_2\{H_1\{x[n] + \sum_{i=1}^r \alpha_i v_i[n]\}\}\dots\}\}. \quad (9)$$

Управление уровнем шумовой составляющей

Управление интенсивностью шумового сигнала производится через отношение сигнал шум, которое определяется следующим выражением

$$SNR = 10 * \log_{10} \left(\frac{P_x}{P_v} \right), \quad (10)$$

где P_x — мощность исходного сигнала, а P_v — мощность шумового сигнала.

Для расчета мощности дискретного сигнала необходимо посчитать среднее значение квадрата отсчетов, для это используется следующее выражение

$$P_x = \frac{1}{N} \sum_{n=0}^{N-1} x^2[n], \quad (11)$$

$$P_v = \frac{1}{N} \sum_{n=0}^{N-1} v^2[n]. \quad (12)$$

Для получения выходного аудиофайла с определенным уровнем SNR, необходимо определить коэффициент масштабирования шума α . Для сгенерированного шумового сигнала коэффициент α определяется выражением

$$\alpha = \sqrt{\frac{P_x}{P_v * 10^{\frac{SNR}{10}}}} \quad (13)$$

Использование формулы 13 позволяет не просто накладывать шумовой сигнал на эталонный, а получать сигнал с контролируемым уровнем отношения сигнал/шум. Это необходимо для последующих исследований, так как один и тот же вариант исходного сигнала может быть преобразован в необходимое количество зашумленных сигналов с контролируемым уровнем шумовой помехи.

Контроль корректности сформированных сигналов

После того как алгоритм заканчивает работу по формированию массива искаженных сигналов необходимо проверить корректность полученных результатов. Такая проверка исключает попадания ошибочных данных в наборы, которые будут использоваться в дальнейших исследованиях.

Одним из параметров для контроля является длительность сигнала. Необходимо чтобы длительность исходного сигнала была равна длительности выходного

$$N_y = N_x. \quad (14)$$

Следующим важным условием является уровень полученного сигнала, в частности отсутствие превышения амплитудой некоторого уровня или же клиппинга. Если сигнал нормализован такое требование можно описать как

$$|y[n]| \leq 1. \quad (15)$$

Если полученный сигнал не удовлетворяет данному требованию он должен быть дополнительно нормализован или исключен из конечного набора.

Для сигналов, к которым применялись шумовые искажения, необходимо проверять итоговый уровень отношения сигнал шум, которое должно быть ниже определенного уровня, задаваемого вручную

$$|SNR_{target} - SNR_{real}| \leq \varepsilon, \quad (16)$$

где SNR_{target} и SNR_{real} — отношение сигнал/шум задаваемое перед началом работы алгоритма и отношение сигнал/шум, которое действительно получается на выходе, а ε — допустимое отклонение.

Заключение

В настоящей работе рассмотрен алгоритм работы генератора тестовых речевых аудиоданных с управляемыми параметрами, влияющими на спектральные и шумовые преобразования. Формализован алгоритм формирования производных аудиоданных на основе эталонного аудиофайла.

Алгоритм описывает математический аппарат шумовых и спектральных преобразований исходного аудиосигнала и их одновременного использования. Для контроля выходных данных определены параметры контроля такие как: длительность сигнала, уровне выходного сигнала и отношения сигнал/шум.

Результаты данной работы могут быть использованы в исследованиях методов шумоподавления, восстановления речи из зашумленных записей, а также в анализе и улучшении систем распознавания речи. Предложенный алгоритм позволяет обеспечить параметризуемость, предсказуемость и повторяемость формирования данных для проведения исследований.

Исследование выполнено при поддержке гранта Российского научного фонда №24-11-00340 (<https://rscf.ru/project/24-11-00340/>).

Литература

1. Козлачков С.Б., Дворянкин С.В., Бонч-Бруевич А.М. Принципы формирования тестовых речевых сигналов при оценках эффективности технологий шумоочистки // Вопросы кибербезопасности. – 2018. – № 3(27). – С. 9-15. DOI: 10.21681/2311-3456-2018-3-09-15.
2. Продеус А.Н. Речевые корпуса: создание и проблемы // Электротехнические и компьютерные системы. – 2013. – № 9(85). – С. 118-126.
3. Столбов М. Б., Зубов Г. Н. Программные средства шумоочистки записей речи // Речевые технологии. – 2014. – № 1-2. – С. 103-113.
4. Петровский А. А., Азаров И. С., Лихачёв Д. С., Ромашкин Ю. Н., Жигулёвцев Ю. Н., Харламов А. А. Шумоподавление на основе перцептуальных алгоритмов спектрального вычитания и обработки сигналов в подпространствах // Речевые технологии. – 2012. – № 4. – С. 4-15.

5. Вишняков И. Э., Масагин М. М., Одинцов О. А., Слюсарь В. В. Методы и алгоритмы шумоочистки звука в реальном времени // Известия высших учебных заведений. Электроника. – 2021. – Т. 26. – № 2. – С. 184-196. DOI: 10.24151/1561-5405-2021-26-2-184-196.
6. Душкин А.В., Волков А.В., Соколовский С.П Устранение интервальной неопределенности при распознавании признаков угроз безопасности информационным телекоммуникационным системам // Системы управления и информационные технологии. – 2007. – № 3 (29). – С. 70-73.

OPERATING ALGORITHM OF A TEST SPEECH SIGNAL GENERATOR WITH ADJUSTABLE NOISE AND SPECTRAL COMPONENTS

stud. Denisov V.D., prof. Dushkin A.V., Oblienko A.V.

National Research University of Electronic Technology

This paper examines an algorithm for generating test speech signals with adjustable noise and spectral components. The proposed method enables the formation of new audio data based on input data to which various types of distortions with predetermined parameters have been applied. This paper focuses on a formal description of the algorithm, which includes preprocessing the source audio files, adding noise components with specified signal-to-noise ratio values, generating tonal interference, applying transformations aimed at changing the signal's spectral characteristics, and simultaneously using the above-described distortions in various combinations. Application of the developed model allows for the generation of test audio files that can be used for subsequent research in areas such as digital speech processing, noise reduction, speech signal restoration, signal-to-noise ratio estimation, distortion classification, and the analysis of the performance of automated speech recognition systems.



РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА АУДИТА СИСТЕМ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ

студ. Душкин А.В., проф. Щербаков В.А.

Национальный исследовательский университет «МИЭТ»

В статье рассмотрено разработанное программное средство с графическим интерфейсом пользователя (GUI) для визуального анализа и автоматизированного аудита политик межсетевого экранирования Check Point. Приложение реализовано на Python с использованием библиотеки PyQt6 для построения интерфейса и взаимодействует с Web API системы управления Check Point для получения информации о правилах безопасности и их проверке. Основное назначение инструмента – облегчить аудит сложных наборов правил брандмауэра за счёт наглядного отображения всех правил и автоматической проверки соответствия заданным критериям безопасности. Разработанное программное обеспечение позволяет в автоматизированном режиме выполнять первичный аудит политик межсетевого экранирования, выявлять потенциальные ошибки и аномалии, предоставлять данные для анализа и оптимизации конфигураций. Это позволяет повысить защищённость информационной инфраструктуры, сократить влияние человеческого фактора и стандартизировать процесс сопровождения правил доступа в корпоративной сети.

В условиях усложняющегося ландшафта угроз информационной безопасности, одним из базовых элементов защиты остаются межсетевые экраны (МЭ). Они обеспечивают разграничение доступа между сегментами сети, фильтрацию трафика и предотвращение несанкционированных взаимодействий. Эффективность межсетевого экранирования при этом напрямую зависит от корректности конфигурации набора правил, определяющих поведение МЭ в различных ситуациях. Статистически подавляющее большинство успешных атак на сетевой периметр происходят не из-за технических уязвимостей в программно-аппаратных решениях, а вследствие ошибок в настройке правил доступа. Так, по данным отраслевых отчётов, до 99% инцидентов связаны с ошибками конфигурации, включая избыточные разрешения, конфликтующие условия или отсутствие строгого принципа минимально необходимого доступа.

Сложность политик межсетевого экранирования, особенно в крупных инфраструктурах, требует применения специализированных программных решений, позволяющих систематизировать правила, выявлять ошибки конфигурации, обнаруживать дублирующие или конфликтующие условия, а также получать визуальные и текстовые отчёты, пригодные для аудита [1, 2]. В связи с этим особую актуальность приобретает задача разработки программного средства, способного выполнять анализ правил МЭ, экспортированных из промышленных решений, и обеспечивать аудит их корректности в автоматизированном режиме.

Целью настоящей работы является создание программного средства для анализа и аудита правил межсетевых экранов с целью выявления ошибок конфигурации и повышения соответствия политике безопасности.

Функциональные требования

Разработка велась на основании перечня функциональных требований, определяющих что именно должно уметь приложение. Приведем основные функциональные возможности инструмента.

Аутентификация и подключение к Check Point Management API: приложение должно предоставить интерфейс для ввода параметров подключения (адрес сервера, учетные данные) и, используя эти данные, установить сессию с сервером управления Check Point. Необходимо подтвердить успешность входа (получение токена сессии) или выдать понятную ошибку при неудаче.

Получение и отображение правил безопасности: после подключения система запрашивает через API актуальный набор правил межсетевого экрана (правила Access Control). Все полученные правила отображаются пользователю в удобочитаемом виде (таблица в приложении). Обязательны к отображению основные атрибуты правил: источники, назначения, сервисы/приложения, действие, состояние (включено/выключено), логирование, комментарии. Желательно также показывать номер правила или идентификатор для однозначной ссылки.

Обновление данных: пользователь должен иметь возможность обновить список правил (например, если параллельно кто-то изменил политику или для повторного аудита).

Выполнение аудита правил: ключевая функция – автоматическая проверка загруженной политики по множеству критериев (см. ниже). Приложение для каждого правила анализирует соответствие правила заданным шаблонам нежелательных конфигураций и формирует перечень обнаруженных несоответствий.

Отображение результатов аудита: результаты проверок выводятся пользователю в структурированном виде (список проблемных правил с пояснениями). Пользователь должен легко видеть, какие правила и почему помечены. Кроме того, должна быть возможность быстро перейти от элемента в списке проблем к соответствующему правилу в общем списке (навигация или подсветка).

Настройка проверок: пользователь (аудитор) может управлять набором выполняемых проверок и их параметрами через специальный интерфейс настроек.

Обработка ошибок и исключений: если в процессе работы происходят сбои – недоступен сервер API, потеряно соединение, получены некорректные данные, внутренние ошибки приложений – эти ситуации должны быть корректно обработаны. Приложение не должно «падать»; вместо этого оно должно уведомить пользователя о проблеме.

Интуитивно понятный интерфейс: пользователю, знакомому с предметной областью (политики брандмауэра), должно быть легко пользоваться инструментом. Это означает логичная организация информации (вкладки, таблицы), использование понятных терминов (на русском языке для отечественных специалистов – «Источник», «Назначение», «Действие» и т.д.), подсказки при наведении на элементы UI, сообщения с описательной информацией. Кроме того, приложение должно предупреждать о длительных операциях (например, при загрузке 1000+ правил – показывать прогресс).

Безопасность: приложение не выполняет изменений на стороне Check Point (только чтение), однако функциональные требования включают безопасное хранение сессионных данных в рамках одного запуска (не выводить лишний раз SID или пароль в логи, очищать пароль после использования). При работе с API желательно использовать минимально необходимые права – то есть, приложение должно работать даже у пользователя с ролью только чтения конфигурации.

Локализация: по требованиям целевой аудитории, интерфейс приложения реализован на русском языке (в примере) для удобства специалистов, не владеющих английским. Однако, функционально желательно отделить текст от кода, чтобы поддерживать многоязычность – это может быть достигнуто через Qt-механизм переводов. В текущей версии достаточно русскоязычного интерфейса.

Экспорт результатов (желательно): инструмент должен позволять сохранить отчет о выявленных проблемах – например, экспортировать список нарушений в файл (CSV, PDF или docx). Это полезно для включения в итоговый отчет аудита или пересылки ответственным администраторам. В базовой реализации достаточно функции копирования текста из вкладки «Аудит» в буфер обмена, либо сохранения простого текстового отчета.

Стоит отметить, что все из перечисленных требований были учтены при проектировании. Некоторые (например, экспорт в PDF) могут быть реализованы на этапе доработки, но заложены как возможность. Главное – приложение выполняет свою функцию: быстро и наглядно выявлять проблемные места в конфигурации брандмауэра.

Архитектурное решение

Рассмотрим подробнее разработанное программное средство с графическим интерфейсом пользователя (GUI) для визуального анализа и автоматизированного аудита политик межсетевого экранирования Check Point. Приложение реализовано на Python с использованием библиотеки PyQt6 для построения интерфейса и взаимодействует с Web API системы управления Check Point для получения информации о правилах безопасности и их проверке. Основное назначение инструмента – облегчить аудит сложных наборов правил брандмауэра за счёт наглядного отображения всех правил и автоматической проверки соответствия заданным критериям безопасности.

Архитектура разрабатываемого приложения основана на принципе клиент-серверного взаимодействия: GUI-приложение выступает в роли клиента к серверу управления Check Point, обращаясь к нему через открытый веб-интерфейс API. Пользователь взаимодействует с интерфейсом PyQt6-приложения, которое через HTTPS-запросы обращается к Web API сервера управления Check Point, получая необходимые данные о политиках безопасности. Сервер управления (Management Server) обрабатывает запросы API и возвращает ответ в формате JSON, содержащий запрошенную информацию (список правил, объекты, статистику и т.д.). Приложение парсит эти данные и отображает их пользователю, а также выполняет локальный анализ (проверки аудита) согласно заложенным правилам. Такой подход позволяет отделить интерфейс и логику проверки от собственно системы безопасности: все взаимодействие происходит через официально поддерживаемый API, без прямого доступа к базам данных Check Point.

Архитектуру внутренней структуры приложения условно можно разделить на несколько модулей (компонентов).

Модуль API-взаимодействия – отвечает за соединение с сервером Check Point и выполнение HTTP(S) запросов к Management API. Этот модуль реализует функции логина, запроса списка правил, объектов и др. через REST API. Взаимодействие происходит путем отправки POST-запросов на эндпоинты API (например, /web_api/login для аутентификации, /web_api/show-access-rulebase для получения правил и т.д.) с передачей данных в формате JSON и получением ответа, также закодированного в JSON. Для последующих запросов после логина используется уникальный токен сессии (SID), передаваемый в заголовке X-chkp-sid – это обеспечивает авторизацию и привязку изменений к текущей административной сессии пользователя.

Модуль бизнес-логики аудита – реализует собственно проверку политик по заданным правилам и критериям. Получив от API структуру правил (список правил с полями: источник, назначение, сервисы/приложения, действие, логирование, примечание, флаги и пр.), данный модуль выполняет серию проверок (о них подробно см. секцию «Проверки аудита правил» ниже). Результаты проверок (найденные несоответствия, потенциальные проблемы в конфигурации) передаются модулю интерфейса для отображения на вкладке аудита.

GUI-модуль – отвечает за отображение информации и взаимодействие с пользователем. Построен на PyQt6 и включает классы окон и виджетов: окно авторизации (входа), главное окно приложения с вкладками, диалоговые окна (например, настройки). GUI-модуль принимает ввод от пользователя (например, введение адреса сервера и учетных данных, нажатие кнопки «Аудит» и др.) и вызывает соответствующие функции API-модуля или модуля логики. Также он получает результаты (список правил, список найденных проблем) и отображает их в удобном виде (таблицы, списки, диалоговые сообщения).

Модуль управления данными (опционально, при достаточной сложности приложения) – может выделяться для хранения локального состояния: списков объектов, результатов аудита, кэша данных между сеансами. В рамках данной реализации основной акцент сделан на прямом отображении полученных от API данных, поэтому роль отдельного слоя данных минимальна – приложение действует как пассивный клиент, не изменяющий данные на сервере (кроме выполнения команд логина и чтения). Тем не менее, для эффективной работы с большим объемом правил можно использовать модель представления данных (например, Qt Model/View), при которой правила загружаются в модель, а UI-виджеты отображают их по мере прокрутки или фильтрации.

Взаимодействие между модулями происходит через четко определенные интерфейсы. GUI вызывает функции API-модуля асинхронно (чтобы не блокировать основной поток интерфейса) и получает результат через сигналы/слоты Qt или коллбэки. Модуль аудита может быть встроен в API-модуль (после получения данных сразу анализирует) либо оформлен отдельно – в данном проекте проверки реализованы внутри приложения, после получения полной базы правил.

Основной сценарий работы: пользователь запускает приложение → вводит адрес сервера управления Check Point, имя пользователя и пароль в окне входа → GUI-модуль вызывает метод API-модуля login() для аутентификации → сервер Check Point получает запрос и возвращает токен сессии (SID) → приложение открывает главное окно и инициирует загрузку правил (например, вызывает get_rulebase) → API-модуль запрашивает у сервера список всех правил политики (возможно, постранично, если правил очень много) → сервер возвращает JSON с правилами → модуль аудита проходит по списку правил и отмечает несоответствия (формирует список обнаруженных проблем) → GUI-модуль обновляет интерфейс: заполняет таблицу правил на вкладке «Все правила» и выводит итоги аудита на вкладке «Аудит». В процессе этого сценария предусмотрена индикация загрузки и обработка ошибок (например, если логин не удался – выводится сообщение об ошибке и главное окно не открывается).

Архитектурное решение предполагает *разделение ответственностей*: взаимодействие с внешней системой (Check Point API) изолировано в отдельном компоненте, что упрощает поддержку (например, при обновлении версии API или смене методов аутентификации изменения локализованы в одном месте). UI отделен от логики проверки – это позволяет модифицировать правила аудита или логику отображения независимо друг от друга. Кроме того, такой дизайн облегчает модульное тестирование: можно тестировать модуль аудита на подготовленных JSON-данных правил без фактического подключения к Check Point, либо эмулировать ответы API.

Пользовательский интерфейс приложения

Пользовательский интерфейс разработан с учетом удобства работы аудитора информационной безопасности или администратора, анализирующего правила брандмауэра. Основные элементы интерфейса включают:

- *окно авторизации* (логина) – стартовое окно, появляющееся при запуске приложения;
- *главное окно с вкладками*: «Все правила» и «Аудит» – основной рабочий экран после входа;
- *диалог настроек проверок* – вызывается из главного окна (например, кнопкой «Настройки» на вкладке аудита или пунктом меню) и позволяет настроить параметры аудита.

Главное окно загружается после успешной аутентификации. Оно построено на основе класса QMainWindow и содержит меню, панель инструментов (при необходимости) и центральную область с вкладками. Название окна отображает имя подключенного сервера или базы политики (например: «AuditTool – Политика Standard_IT (CheckPoint_Server01)» для наглядности). В нижней части может располагаться статус-бар для отображения текущего состояния (например, «Загружено правил: 120», «Аудит выполнен: найдено 5 проблем» или сообщения об ошибках/успехе операций).

Центральная область организована в виде вкладок (QTabWidget), каждая из которых представляет определенный режим работы. Одна из основных – вкладка «Аудит», предназначенная непосредственно для

отображения результатов проверки (аудита) политики на соответствие лучшим практикам и заданным требованиям безопасности (рисунок 1).

Severity	Issues	Layer	Rule #	Rule Name	Source	Destination	Service	Action	Track	Enabled	Comments
Medium	Hit count is zero; Service is Any in Accept Rule	Network	1	First Rules	Multi-Range (address-range, IPv4 Range: 10.0.0.0 - 10.0.0.5; IPv6 Range: F800:1 - F800:5)	Group 3 (group) = [net, 172.24.0.0, 16 (Network, IPv4 Subnet: 172.24.0.0/16); Multi-Range (address-range, IPv4 Range: 10.0.0.0 - 10.0.0.5; IPv6 Range: F800:1 - F800:5; jandel.ru (DNS Domain)); Group 5 with ex (group-with-exclusion, Include Any, Exclude Group 4 (group) = [svr, 2.2.2.2 (Host, IPv4, 2.2.2.2)]]	Any (CpmiAnyObject)	Accept (RulebaseAction)	Log (Track)	True	
High	Hit count is zero; Service is Any in Accept Rule; Source is Any in Accept Rule	Network	2	Second Rule	Any (CpmiAnyObject)	Multi-Range-single (multicast-address-range, IPv4 Range: 224.0.0.1 - 224.0.0.1; Multi-Range-many (multicast-address-range, IPv4 Range: 224.0.0.1 - 224.0.0.24)	Any (CpmiAnyObject)	Accept (RulebaseAction)	Log (Track)	True	
High	Destination is Any in Accept Rule; Hit count is zero	Network	3	Third Rule	Access_rule (Access-rule, Allowed Networks: any, Machines: any, Users: any, Allowed RA Clients: Any); Netfeed (network-feed, Feed type: IP Address, Feed URL: https://test.test.test.nothing, Update interval (s): CPObjsd (dynamic-object))	Any (CpmiAnyObject)	test-svc-group (service-group) = [test-tcp (service-tcp, Port: 4434); test-udp (service-udp, Port: 4434); test-rpc (service-rpc, Program number: 4434); test-dce (service-dce-rpc, Interface UUID: 12345678-1234-abcd-ef00-0123456789ab); test-icmp (service-icmp, ICMP type: 6); test-other (service-other, IP Protocol: 350); test-gtp (service-gtp, Version: v2, Name: 510); test-otp (service-otp, Port: 4434)]	Accept (RulebaseAction)	Log (Track)	True	
High	Hit count is zero; No Track configured	Network	4	Fourth Rule	Any (CpmiAnyObject)	Any (CpmiAnyObject)	Any (CpmiAnyObject)	Inner Layer (Global)	None (Track)	True	
High	Hit count is zero; No Track configured	Network / Layer_2	4.1	Inlayer Rule	svr, 192.168.10.1 (Host, IPv4: 192.168.10.1)	Any (CpmiAnyObject)	Any (CpmiAnyObject)	Inner Layer (Global)	None (Track)	True	
High	Hit count is zero; No Track configured	Network / Layer_2 / Layer_3	4.1.1	Cleanup rule	Any (CpmiAnyObject)	Any (CpmiAnyObject)	Any (CpmiAnyObject)	Drop (RulebaseAction)	None (Track)	True	
High	Hit count is zero; No Track configured	Network / Layer_2	4.2	Cleanup rule	Any (CpmiAnyObject)	Any (CpmiAnyObject)	Any (CpmiAnyObject)	Drop (RulebaseAction)	None (Track)	True	
High	Hit count is zero; No Track configured	Network	5	Fifth Rule	CP_default_Office_Mode_address... (Network, IPv4 Subnet: 172.16.10.0/24)	CP-RS2-SMS (checkpoint-host)	Http (service-tcp, Port: 80); https (service-tcp, Port: 443); HTTP_and_HTTPS_proxy (service-tcp, Port: 8080)	Drop (RulebaseAction)	None (Track)	True	
High	Hit count is zero; No Track configured; Rule configuration is not saved	Network	6	6 Rule	None (CpmiAnyObject)	None (CpmiAnyObject)	None (CpmiAnyObject)	Accept (RulebaseAction)	None (Track)	False	Some Coi

Сводка нарушений:
 High: 1024
 Medium: 2149
 Info: 5

Рисунок 1 – Интерфейс главного окна (вкладка «Аудит») после проведенного аудита

Интерфейс вкладки включает следующие составляющие:

Кнопка «Запустить аудит» (если аудит не выполняется автоматически) или индикатор статуса аудита. После загрузки правил пользователь может нажать эту кнопку, чтобы инициировать проверку. Впрочем, в реализации возможно автоматическое выполнение аудита сразу после получения правил – тогда результаты появляются без дополнительных действий. Тем не менее, кнопка «Обновить аудит» полезна для повторного запуска проверки, например, если настройки проверок были изменены.

Кнопка «Настройки проверок...» – открывает диалог настроек аудита (описан далее), где можно включать/отключать определенные проверки или менять параметры. После закрытия диалога пользователь обычно заново запускает аудит, чтобы применить новые настройки.

Область вывода результатов аудита. Это может быть многострочный текстовый протокол, но удобнее использовать структурированное представление. В варианте реализации – список или дерево (QTreeWidget или QListWidget) с перечислением найденных проблем.

Статистика аудита. В нижней части вкладки или в отдельном блоке может кратко отображаться сводка: «Проверено правил: N. Найдено проблем: X критических, Y предупреждений.» Это помогает сразу оценить общий «балл» политики. В более продвинутом варианте можно вычислять процент соответствия или рейтинг политики на основе веса различных проверок – однако в данном разработанном инструменте реализована простая количественная оценка (число выявленных проблем по категориям).

Если политика соответствует всем проверкам (нет нарушений), то вкладка «Аудит» отобразит сообщение «Проблем не обнаружено: политика соответствует заданным требованиям.» Возможно, это сопровождается зелёной галочкой. Пользователь в таком случае может быть уверенным, что по заложенным метрикам политика «чиста».

Таким образом, разработанное в рамках данной работы средство позволяет в автоматизированном режиме выполнять первичный аудит политик межсетевого экранирования, выявлять потенциальные ошибки и аномалии, предоставлять данные для анализа и оптимизации конфигураций. Это позволяет повысить защищённость информационной инфраструктуры, сократить влияние человеческого фактора и стандартизировать процесс сопровождения правил доступа в корпоративной сети.

Литература

- Markin P.V., Dushkin A.V., Kochedykov S.S. Express assessment method for the risk of impaired functional stability information and communication system in conditions cyber attacks // Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus 2019), Saint

Petersburg — Moscow, 28-30 января 2019 года. – Saint Petersburg — Moscow: Institute of Electrical and Electronics Engineers Inc., 2019. – P. 1754-1757. – DOI: 10.1109/EIConRus.2019.8657323.

2. Громов Ю.Ю., Карасев П.И., Коршунов Д.С., Ершов Н.С. Аудит информационной безопасности АСУ // Промышленные АСУ и контроллеры. – 2023. – №3. – С. 30-36. – DOI: 10.25791/asu.3.2023.1424.

DEVELOPMENT OF A SOFTWARE TOOL FOR AUDIT OF FIREWALL SYSTEMS

stud. Dushkin A.V., prof. Shcherbakov V.A.

National Research University of Electronic Technology

This article describes a software tool developed with a graphical user interface (GUI) for visual analysis and automated auditing of Check Point firewall policies. The application is implemented in Python using the PyQt6 library for the interface and interacts with the Check Point management system's Web API to retrieve information about security rules and their verification. The tool's primary purpose is to facilitate the audit of complex firewall rule sets by clearly displaying all rules and automatically checking for compliance with specified security criteria. The developed software enables automated initial audits of firewall policies, identifies potential errors and anomalies, and provides data for configuration analysis and optimization. This improves the security of the information infrastructure, reduces the impact of human error, and standardizes the process of maintaining access rules on the corporate network.



ОБ ОБОСНОВАННОСТИ ИСПОЛЬЗОВАНИЯ МЕТОДОВ И ИНСТРУМЕНТОВ ЦИФРОВОЙ КРИМИНАЛИСТИКИ НА ОСНОВЕ КЛАССИФИКАЦИИ ИСТОЧНИКОВ ЦИФРОВЫХ СЛЕДОВ

студ. Шкилевич Н.Н.

Национальный исследовательский университет «МИЭТ»

В статье рассматриваются методы и инструменты цифровой криминалистики при расследовании инцидентов информационной безопасности. Актуальность работы обусловлена ростом киберпреступлений и необходимостью обеспечения юридической значимости цифровых доказательств. Проведён анализ нормативно-правовой базы РФ и международных стандартов (MITRE ATT&CK, NIST SP 800-86). Предложена постановка задачи классификации источников цифровых следов по месту хранения для обоснованного выбора методов и средств их извлечения. Результаты направлены на повышение достоверности и воспроизводимости цифровых расследований.

За последнее время наблюдается устойчивый рост числа преступлений, связанных с использованием компьютерных технологий. Это стимулирует развитие новых инструментов и методик, направленных на помощь аналитикам киберинцидентов в установлении обстоятельств совершения преступления, включая определение субъекта, способа и последовательности его действий. В результате сформировалась компьютерная и сетевая криминалистика, обеспечивающая корректное выявление, анализ и представление цифровых доказательств в рамках судебных разбирательств.

Вместе с тем усложнение инфраструктуры информационных систем и увеличение объема обрабатываемых данных приводят к росту требований к качеству и обоснованности проводимых расследований. Анализ инцидентов требует обработки больших массивов разнородной информации, что повышает вероятность ошибок и искажений при отсутствии формализованных подходов. В этих условиях особую значимость приобретает необходимость регламентации методов цифровой криминалистики и используемых инструментов.

Таким образом, актуальность исследования обусловлена необходимостью формирования стандартизированных и воспроизводимых подходов к проведению цифровых расследований, обеспечивающих достоверность результатов и их юридическую значимость. Применение международных стандартов и развитие единых методик позволяют минимизировать указанные риски и повысить эффективность как технического анализа, так и последующего использования его результатов в правоприменительной практике.

В Российской Федерации цифровая криминалистика развивается на пересечении с судебной экспертизы, информационной безопасности, аудита и финансового контроля. При этом её правовое регулирование носит фрагментарный характер и основывается на ряде нормативно-правовых актов, регулирующих смежные области.

Ключевым документом является Федеральный закон № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации», который определяет общие принципы проведения судебных экспертиз, требования к экспертам, а также порядок организации экспертной деятельности. Однако он не учитывает специфику цифровых доказательств и методов их обработки. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации» регулирует отношения, связанные с использованием информации и обеспечением её защиты. В контексте цифровой криминалистики он задаёт общие требования к обращению с информацией, но не описывает процедуры её криминалистического исследования. Федеральный закон № 402-ФЗ «О бухгалтерском учёте» и Федеральный закон № 115-ФЗ «О противодействии легализации доходов, полученных преступным путём» применяются в случаях расследования финансовых и корпоративных инцидентов. Они определяют требования к фиксации, хранению и анализу финансовой информации, которая может выступать в качестве цифровых доказательств.

Существующая нормативно-правовая база в Российской Федерации охватывает лишь общие аспекты судебной экспертизы и обращения с информацией. При этом отсутствует специализированное регулирование, описывающее процесс цифровой криминалистики, включая методы сбора, анализа и фиксации цифровых следов, а также требования к инструментам, применяемым при расследовании. Это приводит к необходимости использования международных стандартов для разработки обоснованности использования тех или иных методик и средств цифровой криминалистики.

Установление единых мировых практик позволяет привлечь большее количество специалистов и принять в рассмотрение нюансы проведенных исследований, что позволяет сформировать качественное представление об области цифровой криминалистики. Результаты работы могут быть применимы организациями, владеющими информационными ресурсами, для совершенствования технологий сбора и

обработки информации, способствующей проводить эффективное расследование инцидентов информационной безопасности.

В рамках модели MITRE ATT&CK [1] кибератака рассматривается как последовательность взаимосвязанных этапов, отражающих жизненный цикл действий нарушителя от подготовки до достижения конечной цели. Криминалистическое расследование позволяет найти следы атакующего. Исходя из того, что след остается в любом случае, необходимо рассмотреть процесс расследования подробнее. Независимо от ситуации, процесс криминалистического исследования включает основные этапы: сбор информации, проведение экспертизы, анализ результатов экспертизы, предоставление результатов [2]. Данный подход соответствует рекомендациям NIST SP 800-86, описывающего интеграцию криминалистических методов в процессы реагирования на инциденты и устанавливающего базовую модель проведения цифровых расследований.

Наличие стандартов не позволяет избежать проблем, связанных с верификацией цифровых доказательств в суде. Как указывает Е. Casey в своих трудах [3] верификация представляет собой серьезную методологическую задачу, поскольку следователю и суду зачастую недоступна возможность проверить корректность работы алгоритмов, формирующих такие следы.

Решение проблемы недоверия суда к цифровым доказательствам возможно при формировании комплексного подхода, включающего разработку и внедрение верифицированных алгоритмов сбора и обработки цифровых следов, а также строгую регламентацию использования инструментов цифровой криминалистики. Верификация алгоритмов предполагает доказательство их корректности, воспроизводимости и неизменности результатов при одинаковых входных данных, что позволяет снизить влияние скрытых ошибок и повысить доверие к получаемым результатам.

Не менее важным является установление требований к инструментам цифровой криминалистики, включая их сертификацию, тестирование и документирование принципов работы. Прозрачность используемых средств, возможность независимой проверки их функциональности и наличие утвержденных методик применения позволяют обеспечить проверяемость результатов экспертизы со стороны суда и других участников процесса.

Кроме того, необходима формализация процедур фиксации и обработки цифровых доказательств, включая описание всех этапов работы с данными, ведение журналов действий и соблюдение цепочки хранения улик. Это обеспечивает прослеживаемость происхождения доказательств и исключает возможность их изменения или искажения.

В связи с обширностью области цифровой криминалистики возникает необходимость сгруппировать инструменты и методы получения цифровых следов. Для решения этого вопроса необходима классификация, которая может проводиться [4] по месту фиксации, способу образования, содержательной направленности. Для решения проблемы необходимо так же проводить классификацию по типу источников получаемых данных. Основное отличие от классификации по месту фиксации заключается в том, что необходимо рассматривать среды, из которых собираются данные. Данные представляют собой информацию, которая представлена в цифровом виде и записана на определенный хранилище. Он может быть энергозависимым или наоборот энергонезависимым. В зависимости от этого меняется процедура получения данных. Так же необходимо понимать, что для удобства восприятия данные представляют из себя файлы, записанные при использовании принципов кодирования. Это позволяет разделить источники данных на подкатегории: текстовая информация, информация, представленная в виде изображений.

Для формирования критериев оценивания инструментов и методов проведения цифровой криминалистики необходима постановка задач дальнейшего исследования. Основная задача заключается в классификации источников цифровых следов и соответственное разделение инструментов цифровой криминалистики. В дальнейшем это позволит унифицировать требования к инструментам, позволив выделить и сертифицировать те из них, которые позволяют достичь принятие этих средств в суде как единственно правильные. Задача формализации процесса сбора и анализа данных, что подразумевает документирование и сохранение источников данных для возможности повторить результаты при равных исходных. Это позволяет повысить достоверность полученных результатов и обосновать правильность сделанных выводов.

В работе проанализированы методы и инструменты цифровой криминалистики при расследовании инцидентов информационной безопасности. Показано, что нормативно-правовая база Российской Федерации не содержит специализированного регулирования процессов сбора, анализа и фиксации цифровых следов, что снижает юридическую значимость цифровых доказательств.

На основе изучения модели MITRE ATT&CK и рекомендаций NIST SP 800-86 предложена постановка задачи классификации источников цифровых следов по месту их хранения и типу данных. Такая классификация позволит систематизировать методы и инструменты цифровой криминалистики,

обоснованно выбирать средства извлечения данных, повысить воспроизводимость результатов и укрепить доверие суда к цифровым доказательствам.

Разработка предложенной классификации является важным шагом к формированию стандартизированных и юридически состоятельных подходов к проведению цифровых расследований.

Литература

1. MITRE ATT&CK: база знаний тактик и техник кибератак [Электронный ресурс]. – Режим доступа: <https://attack.mitre.org> (дата обращения: 20.04.2026).
2. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response [Электронный ресурс]. – Gaithersburg: National Institute of Standards and Technology, 2006. – Режим доступа: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf> (дата обращения: 20.04.2026).
3. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Academic Press, 2011, 807 p
4. Родивилина В.А., Коломинов В.В. Электронно-цифровые следы как доказательства при расследовании интернет-мошенничеств: криминалистические и процессуальные аспекты вестник восточно-сибирского института мвд россии. 2026. № 1 (116). с. 214-227.

TASK STATEMENT FOR JUSTIFYING THE USE OF DIGITAL FORENSICS METHODS AND TOOLS BASED ON THE CLASSIFICATION OF DIGITAL EVIDENCE SOURCES

stud. Shkilevich N. N.

National Research University of Electronic Technology

The paper examines digital forensics methods and tools used in investigating information security incidents. The relevance of the work stems from the rise in cybercrimes and the need to ensure the legal admissibility of digital evidence. An analysis of the Russian regulatory framework and international standards (MITRE ATT&CK, NIST SP 800-86) has been conducted. A task statement is proposed for classifying digital evidence sources based on storage location to enable the justified selection of methods and tools for their extraction. The results are aimed at improving the reliability and reproducibility of digital investigations.



КОГНИТИВНЫЕ ИСКАЖЕНИЯ СПЕЦИАЛИСТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАССЛЕДОВАНИИ ИНЦИДЕНТОВ

доц., к.м.н. Калищук С. А., студ. Жукова А. А.

Национальный исследовательский университет «МИЭТ»

В статье анализируются когнитивные искажения, систематически проявляющиеся в профессиональной деятельности аналитиков центров операций безопасности (SOC). На основе обобщения данных когнитивной психологии, отраслевых отчётов и эмпирических исследований выделены пять основных типов когнитивных ошибок: преждевременное закрытие версии расследования, эффект подтверждения, усталость от оповещений, недооценка угрозы внутреннего нарушителя и слепое доверие автоматизированным корреляциям систем SIEM. Приводятся статистические данные и результаты исследований. Предложены практические меры противодействия.

Введение

Расследование инцидентов информационной безопасности традиционно рассматривается преимущественно как технический процесс, направленный на выявление атаки, сбор доказательной базы и атрибуцию действий злоумышленника. Однако за техническими аспектами часто скрывается значимый фактор, существенно осложняющий процесс, – когнитивные ограничения человеческого мышления аналитика [1, 2].

Когнитивная психология на протяжении нескольких десятилетий изучает систематические отклонения мышления от норм рациональности [3, 4]. В сфере информационной безопасности данные явления остаются недостаточно исследованными: отсутствуют стандартизированные методики оценки качества аналитической работы, а образовательные программы подготовки специалистов редко включают модули, посвящённые человеческому фактору [5]. Так как обычно информационная безопасность чаще всего делает акцент на работе с техникой и программными решениями, что редко ассоциируется с настройкой человеческого поведения и влияния самих людей на результат в целом. Тем не менее, именно когнитивные искажения нередко становятся причиной серьёзных ошибок при расследовании инцидентов и оценке рисков.

Цель настоящей работы – систематизация пяти ключевых когнитивных искажений, наиболее характерных для деятельности аналитиков SOC, на основе эмпирических данных, а также разработка научно обоснованных рекомендаций по их минимизации.

1. Преждевременное закрытие версии расследования

Преждевременное закрытие версии представляет собой когнитивную ошибку, при которой аналитик прекращает дальнейшее расследование, как только первая гипотеза представляется достаточно правдоподобной. В основе этого феномена лежит естественное стремление мозга к когнитивной экономии: подтверждение первоначальной догадки дает ощущение завершенности, тогда как поиск альтернатив требует значительных ментальных усилий. Аналитик бессознательно игнорирует сигналы, не вписывающиеся в первую версию, что создает иллюзию исчерпывающего анализа. Наиболее часто эта ошибка возникает в условиях дефицита времени, информационной перегрузки или при работе с рутинными, «типичными» случаями. Чем выше опыт аналитика, тем больше риск: автоматизмы профессионального мышления ускоряют постановку первого диагноза, но одновременно подавляют критическую рефлекссию. Ключевой триггер – субъективное ощущение, что собранных данных «достаточно», хотя объективно они могут объяснять лишь часть симптомов. В медицинской диагностике аналогичное явление, именуемое «диагностическим закрытием», относится к числу ведущих причин врачебных ошибок [6].

Типичный сценарий и реальный пример. Аналитик фиксирует попытку подбора паролей с использованием известного инструмента (например, Mimikatz) и закрывает инцидент как «атака методом brute-force». Аналогичная ситуация наблюдалась в ряде расследований, когда первоначальная классификация как «commodity malware» приводила к игнорированию признаков настойчивости и сложной APT-атаки даже при появлении дополнительных индикаторов [7].

Меры противодействия: внедрение обязательных контрольных чек-листов при закрытии инцидентов, проведение регулярных ретроспективных разборов закрытых дел с обязательным поиском пропущенных артефактов.

2. Эффект подтверждения

Эффект подтверждения заключается в тенденции искать, интерпретировать и отдавать предпочтение информации, подтверждающей уже сформированную гипотезу, при одновременном игнорировании или недооценке противоречащих данных. Данное искажение работает автоматически, неосознанно, создавая у аналитика иллюзию исчерпывающей объективности. Исследования показывают, что даже обладая полным

набором фактов, человек под влиянием эффекта подтверждения оценивает подтверждающие его версию свидетельства как более веские и достоверные по сравнению с теми же самыми данными, но представленными как опровергающие гипотезу. В расследовании инцидентов это приводит к туннельному видению: проверяются только очевидные версии, «неудобные» вопросы не задаются, противоречащие показания перепроверяются с меньшей тщательностью. Данное искажение относится к числу наиболее деструктивных в процессе расследования инцидентов [2, 3].

Типичный сценарий и реальный пример. При обнаружении аномальной активности на рабочей станции системного администратора аналитик сосредоточивается исключительно на поиске подтверждающих свидетельств в журналах Active Directory, игнорируя возможный фишинговый вектор и аномалии на других узлах сети. Подобное поведение отмечалось при расследовании инцидентов, когда команды SOC продолжали искать только индикаторы фишинга, игнорируя логи и последующие действия. В случае с SolarWinds (2020) многие организации слишком долго придерживались первоначальной гипотезы о компрометации поставщика, игнорируя противоречащие сигналы [7].

Меры противодействия: применение структурированного метода «advocatus diaboli» (обязательная формулировка альтернативных гипотез на каждом этапе), организация парного анализа инцидентов двумя аналитиками. По данным исследований, такой подход снижает проявления эффекта на 30-40 % [6].

3. Усталость от оповещений

Усталость от оповещений является одним из наиболее изученных и распространённых поведенческих нарушений в центрах операций безопасности [8]. В таблице 1 приведена статистика показателей усталости от оповещений.

Таблица 1

Ключевые статистические показатели усталости от оповещений (2024–2025 гг.)

Показатель	Значение	Источник
Доля организаций, считающих ложные срабатывания главной проблемой обнаружения	73 %	SANS Detection & Response Survey, 2025 [8]
Доля команд, не успевающих обрабатывать поступающий объём оповещений	66 %	SANS, 2024–2025 [8]
Среднесуточный объём оповещений в крупных организациях	2000–10 000+	Отраслевые отчёты [9]
Доля оповещений, остающихся без расследования	40–63 %	Trend Micro, SANS [8, 9]
Доля рабочего времени, затрачиваемого на ложные срабатывания	25–40 %	Trend Micro, SANS [9]

Реальный пример. В инцидентах Equifax (2017) и SolarWinds (2020) команды SOC получали предупреждения об аномальной активности, однако из-за высокого объёма ложных срабатываний и усталости аналитики либо игнорировали их, либо классифицировали как шум, что позволило атакам развиваться в течение длительного времени [10].

Меры противодействия: Совершенствование правил корреляции, внедрение технологий UEBA и SOAR, контекстная приоритизация оповещений, ротация обязанностей аналитиков и ограничение продолжительности смен в режиме интенсивного мониторинга [8].

4. Недооценка внутреннего нарушителя как источника риска

Данный феномен связан с психологическим механизмом внешнего атрибутирования, в результате которого аналитики подсознательно сосредоточивают внимание на внешнем периметре и недооценивают риски, исходящие от сотрудников организации [10]. Действие этого механизма таково: при возникновении инцидента или угрозы мозг автоматически предлагает объяснение, связанное с внешними, а не внутренними причинами, поскольку такое объяснение требует меньшего пересмотра сложившихся представлений о коллективе и собственной компетентности. Как следствие, меры предотвращения инцидентов выстраиваются вокруг внешних барьеров (контроль доступа, межсетевое экранирование, охрана), в то время как мониторинг действий персонала, разделение привилегий и поведенческий анализ остаются недоразвитыми. Преодоление этого искажения требует специальных процедур, предписывающих при каждом анализе инцидента в обязательном порядке формулировать как минимум одну версию с участием внутренних нарушителей. Так, в исследованиях инцидентов информационной безопасности выявлено, что при опросе специалистов о причинах утечек данных в собственных компаниях внешним факторам (взлом,

вирусная атака) придаётся в среднем втрое больше веса, чем при анализе аналогичных инцидентов в сторонних организациях. При этом до 70% расследований, начатых с версии о внешнем нарушителе, на поздних этапах обнаруживают причастность инсайдера, но первоначальный фокус на внешнем периметре приводит к потере следов и несвоевременному принятию мер.

Реальный пример. В ряде крупных инцидентов (включая утечки данных в Verizon и других компаниях) аналитики фокусировались на внешних угрозах, упуская признаки злоупотребления привилегиями или ошибок инсайдеров, что приводило к длительному развитию инцидента [4, 12].

Меры противодействия: Регулярное проведение поиска угроз без предварительных гипотез, внедрение профилей поведения пользователей (UEBA), строгое соблюдение принципа минимальных привилегий и постоянный мониторинг привилегированных учётных записей [11].

5. Слепое доверие СИЕМ-корреляциям

Слепое доверие результатам работы систем SIEM приводит к тому, что аналитик воспринимает корреляционные правила как истину, а не как рабочую модель реальности [11]. В основе этого феномена лежит автоматизация с эффектом ореола: компьютерная система, генерирующая структурированные алерты, воспринимается как объективная и свободная от человеческих ошибок, в отличие от «ненадёжного» сотрудника. При этом аналитик перестаёт критически оценивать, какие именно события и на каких основаниях были включены в корреляцию, какие данные могли быть отфильтрованы на этапе сбора, и какой процент ложноположительных срабатываний заложен в настройках правил. Система превращается из инструмента в авторитетный источник. В таблице 2 приведена распространенность искажения автоматизации.

Таблица 2

Распространённость искажения автоматизации в SOC (2024–2025 гг.)

Вид когнитивного искажения	Распространённость	Источник	Основные последствия
Искажение автоматизации (Automation Bias)	47 %	Hagen et al., 2025 [11]	Недостаточная верификация
Эффект подтверждения по отношению к автоматизации	37 %	Hagen et al., 2025 [11]	Игнорирование противоречащих данных
Самоуспокоенность (Complacency)	высокая	Tilbury, 2024 [12]	Снижение проактивного анализа

Реальный пример. Во многих расследованиях аналитики, получив корреляционное срабатывание SIEM, считали инцидент «разобраным» и не проводили дополнительный анализ контекста (события до и после), что приводило к пропуску Living-off-the-Land техник и сложных APT-кампаний [13].

Меры противодействия: чёткое разграничение ответственности (SIEM формирует гипотезы, аналитик проводит полноценное расследование в полном контексте), регулярная калибровка корреляционных правил совместно с подразделением Threat Intelligence, проведение учений Red Team / Purple Team [5, 13].

Заключение

Когнитивные искажения специалистов информационной безопасности представляют собой закономерное следствие особенностей профессиональной деятельности [1, 3]. Рассмотренные пять типов искажений формируют системную картину уязвимостей аналитического процесса. Преодоление данных искажений возможно посредством внедрения структурированных организационных практик: обязательных чек-листов, метода «advocatus diaboli», парного анализа, гипотезно-ориентированного Threat Hunting и непрерывного совершенствования автоматизированных систем.

Осознание собственных когнитивных ограничений следует рассматривать как важный признак профессиональной зрелости аналитика и необходимое условие построения эффективных и устойчивых процессов расследования инцидентов информационной безопасности.

Литература

1. Валлас Б., Клайн Г. Что мешает принимать решения. – М. : Альпина Паблишер, 2012. – 240 с.
2. Канеман Д. Думай медленно... решай быстро / пер. с англ. А. Андреева. – М. : АСТ, 2014. – 653 с.
3. Kahneman D. Thinking, Fast and Slow. – New York : Farrar, Straus and Giroux, 2011. – 499 p.

4. Verizon 2025 Data Breach Investigations Report. – Basking Ridge : Verizon Business, 2025. – URL: <https://www.verizon.com/business/resources/reports/dbir/> (дата обращения: 06.05.2026).
5. Зельдин С. Э. Методы обнаружения инцидентов ИБ и реагирования на них. – М. : ДМК Пресс, 2023. – 312 с.
6. Groopman J. How Doctors Think. – Boston : Houghton Mifflin, 2007. – 307 p.
7. Overcoming Biases in Cyber Security Problem Analysis // Cybersecurity Magazine. – 2026. – URL: <https://cybersecurity-magazine.com> (дата обращения: 06.05.2026).
8. SANS Institute 2025 Detection & Response Survey. – Bethesda : SANS Institute, 2025. – URL: <https://www.sans.org> (дата обращения: 06.05.2026).
9. Trend Micro SOC Alert Fatigue Report 2025. – Irving : Trend Micro, 2025. – URL: <https://www.trendmicro.com> (дата обращения: 06.05.2026).
10. Cyjax. How to Solve the Problem of Alert Fatigue. – London : Cyjax, 2025. – URL: <https://www.cyjax.com> (дата обращения: 07.05.2026).
11. ASIS International. Uncovering Cognitive Biases in Security Decision Making. – Alexandria : ASIS International, 2022. – URL: <https://www.asisonline.org> (дата обращения: 07.05.2026).
12. Dark Reading : [сайт]. – URL: <https://www.darkreading.com> (дата обращения: 07.05.2026).
13. Hagen R. A. [et al.] Human Factors in AI-Driven Cybersecurity // Proceedings of the Cybersecurity Research Conference. – 2025. – URL: (дата обращения: 07.05.2026).
14. Tilbury J. Automation Bias and Complacency in Security Operation Centres // Computers. – 2024. – Vol. 13. – URL: <https://www.mdpi.com/journal/computers> (дата обращения: 07.05.2026).

COGNITIVE BIASES OF INFORMATION SECURITY SPECIALISTS IN INCIDENT INVESTIGATION

Ph.D., ass. prof. Kalishchuk S. A., stud. Zhukova A.A.

National Research University of Electronic Technology

This article analyzes cognitive biases systematically observed in the professional work of security operations center (SOC) analysts. Based on a synthesis of cognitive psychology data, industry reports, and empirical studies, five main types of cognitive biases were identified: premature closure of events, confirmation bias, alert defense, underestimation of the insider threat, and blind defense with portable SIEM systems. Statistical data, research results, and case studies are provided. Practical countermeasures are proposed.



О ВЛИЯНИИ ОГРАЖДАЮЩИХ КОНСТРУКЦИЙ НА СПЕКТР РЕЧЕВОГО СИГНАЛА ПРИ ОЦЕНКЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ КАНАЛУ

доц., к.т.н., Иванов А.В., асс. Филимонова С.Р.

Новосибирский государственный технический университет

В статье рассматриваются вопросы, касающиеся оценки защищенности акустической речевой информации от утечки по техническим каналам, а именно, оценка влияния различных частотных характеристик затухания ограждающих конструкций на усредненный спектр речевого сигнала и на результат показателя защищенности (разборчивости речи). Построены зависимости разборчивости речи от отношения сигнал шум для случая использования в качестве маскирующей помехи белого шума и измененных под воздействием ограждающих конструкций спектров речевого сигнала. В качестве ограждающих конструкций были рассмотрены: дверь, стена, вентиляция. Произведены необходимые для оценки разборчивости речи измерения. Результаты показывают на необходимость учета частотных характеристик звукоизоляции ограждающих конструкций в вопросе оценки защищенности помещений от утечки речевой акустической информации по техническим каналам.

При проведении закрытых переговоров необходимо обеспечить защищенность акустической речевой информации в помещении от утечки по техническим каналам. Для оценки акустических и вибрационных каналов чаще всего используется частный случай подхода, разработанного Н.Б. Покровским [1], адаптированным для использования в задачах защиты информации [2], заключающиеся в проведении ряда измерений акустических и вибрационных сигналов, и дальнейшего расчета разборчивости речи, который и принимается в качестве показателя защищенности. При проведении измерений чаще всего в качестве тестового сигнала используются акустически шумоподобные сигналы, октавные уровни в частотных полосах которого по методике сопоставляются с аналогичными уровнями усредненного спектра речевого сигнала. Пример значений уровней акустического давления в октавных полосах усредненного спектра речи для интегрального уровня 70 дБ приведен в таблице 1.

Таблица 1.

Значения уровней в октавных полосах для усредненного спектра речи.

Среднегеометрическая частота октавной полосы, Гц	125	250	500	1000	2000	4000	8000
Усредненный спектр речи Н.Б. Покровского, дБ	53	66	66	61	56	53	49

Исследования достоверности применения данной и других подобных методик производятся многими коллективами авторов [3-6]. В большинстве экспериментов исследуются речевые сигналы, записанные от различных дикторов или усредненные спектры речи при наложении маскирующих шумов от средств активной защиты (САЗ). Но, следует отметить, что схема оценки защищенности выглядит следующим образом (рисунок 1). На тестовый сигнал, до его измерения шумомером влияет не только наложение маскирующей помехи от САЗ, но и ограждающая конструкция (ОК). Каждая ОК уникальная и обладает своей частотной характеристикой затухания сигнала при прохождении.

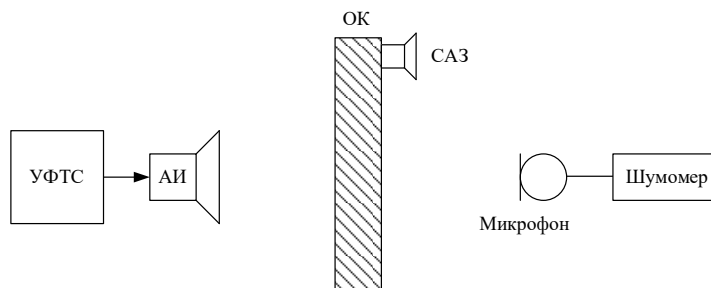


Рисунок 1. Схема проведения оценки защищенности по акустическому каналу.

Где: УФТС – устройство формирования тестового сигнала, АИ – акустический излучатель, САЗ – средство активной защиты, ОК – ограждающая конструкция

Проведем исследование влияния различных ограждающих конструкций на спектр речевого сигнала, а также влияния данных изменений на результаты расчета разборчивости речи по методике [1]. Для примера рассмотрим несколько типовых ограждающих конструкций:

- дверь;

- стена;
- вентиляция.

Проведем измерение значения затухания сигнала при прохождении через данные конструкции, на основании полученных значений затухания оценим влияние ОК на спектр речевого сигнала. Рассмотрим случай применения в САЗ одного из типовых шумов – белого шума. Произведем расчет изменения разборчивости речи от отношения сигнал шум для указанных вариантов конструкций, который предварительно покажет степень влияния ОК на результаты расчетов.

Также примеры значений затухания различных ограждающих конструкций возможно взять в различных стандартах и справочниках, например в [7].

Ранее в работе по оценке влияния различий в спектрах речи дикторов мы уже приводили подробное описание измерительной установки, хорошо себя зарекомендовавшей в подобных исследованиях [8]. Основу установки составляет измерительное сигма-дельта АЦП для акустики LTR24-2 и микрофон ZT-333 с предусилителем P410. Подобное сочетание позволяет использовать для записи сигналов измерительные микрофоны, а также автоматизировать обработку полученных сигналов и необходимые последующие расчеты.

Схема измерения будет соответствовать рисунку 1. Измеряться будет акустическое давление сигналов в дБ относительно 20мкПа. Измеряемые уровни:

- тестового сигнала;
- фонового шума;
- сигнала и шума за ограждающей конструкцией.

Результаты измерений приведены в таблице 2, где $L_{\text{тест}}$ – уровни тестового сигнала, $L_{\text{ш}}$ – уровни фонового шума, $L_{\text{с+ш}}$ – уровни сигнала и шума за ограждающей конструкцией.

Таблица 2.

Результаты измерения уровней в октавных полосах тестового сигнала, фонового шума и смеси сигнала и шума за ограждающими конструкциями

№ октавы	f, Гц	$L_{\text{тест}}$, дБ	ограждающая конструкция					
			дверь		стена		вентиляция	
			$L_{\text{ш}}$, дБ	$L_{\text{с+ш}}$, дБ	$L_{\text{ш}}$, дБ	$L_{\text{с+ш}}$, дБ	$L_{\text{ш}}$, дБ	$L_{\text{с+ш}}$, дБ
1	125	80,4	34,5	59,1	32,9	44,5	40,4	53,5
2	250	84,3	29,3	61,8	28,1	45,8	37,1	54,0
3	500	87,3	28,7	59,8	28,1	47,9	30,2	52,0
4	1000	94,0	25,2	61,3	22,7	44,3	27,2	51,9
5	2000	93,4	24,6	69	22,1	38,5	23,5	59,9
6	4000	88,4	23,2	59,8	23,9	31,7	22,7	49,5
7	8000	83,8	24,2	46,7	24,2	24,9	24,1	33,0

Отметим, что уровень тестового сигнала заведомо задается выше уровней усредненного спектра речи. Данный подход используется для повышения достоверности результатов измерений уровня сигнала за ОК на уровне фоновых шумов и под воздействием затухания. В дальнейшем при оценке защищенности учитывается уровень превышения тестового сигнала в каждой октавной полосе над значениями уровней усредненного спектра речи.

В результате расчетов были получены значения уровней речевого сигнала с учетом частотной характеристики затухания ОК. Значения приведены в таблице 3. Для удобства сравнения все спектры приведены к интегральному уровню 70 дБ.

Таблица 3.

Результаты расчета спектров речи с учетом затухания от ограждающей конструкции в сравнении с усредненным спектром речи

№ октавы	f, Гц	ограждающая конструкция			$L_{\text{тест}}$, дБ
		дверь	стена	вентиляция	
		$L_{\text{с}}$, дБ	$L_{\text{с}}$, дБ	$L_{\text{с}}$, дБ	
1	125	56,5	56,6	58,5	53
2	250	68,3	67,1	68,2	66

3	500	63,3	66,2	63,2	66
4	1000	53,1	51	51,5	61
5	2000	56,4	40,7	55,1	56
6	4000	49,2	35,2	46,7	53
7	8000	36,7	21,5	30,2	49

Для предварительной оценки влияния возможной разницы в спектрах сигналов за ограждающей конструкцией (с учетом частотной характеристики затухания) на оценку защищенности проведем расчет по методике [1] в случае использования в качестве маскирующей помехи белого шума, но заменив усредненный спектр речи значениями полученных спектров. Результаты отражены на графике зависимости разборчивости речи (W) от отношения сигнал/шум (ОСШ) (рисунок 2).

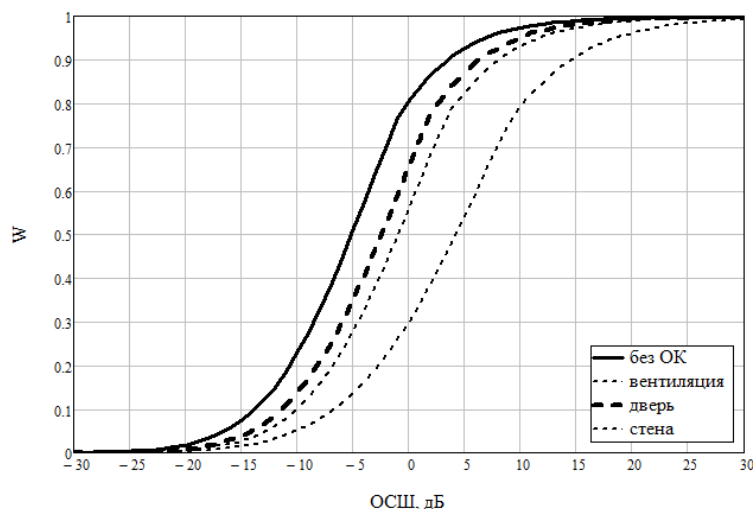


Рисунок 2. Расчетная зависимость разборчивости речи от ОСШ для случая использования в качестве тестового сигнала: усредненного спектра речи (график «без ОК»); спектра речи, полученного на выходе вентиляции; спектра речи, полученного за дверью; спектра речи, полученного за стеной.

Исходя из полученных результатов можно сделать выводы о теоретическом влиянии искажения спектра речи при прохождении через ограждающую конструкцию на результат оценки разборчивости речи по методике. В наиболее значимом для задач защиты информации диапазоне значений разборчивости речи $W < 0.5$ разница в результатах оценки может достигать 0.45, что очень существенно. Также следует отметить, что во всех рассмотренных примерах учет искаженного спектра по сравнению с усредненным привел к снижению разборчивости речи, что для задач защиты информации является положительным эффектом, но также значит, что в подобной ситуации было бы рационально существенно скорректировать уровень маскирующей помехи, снизив тем самым эффект влияния паразитного шума от САЗ в помещении. Полученные результаты основаны только на теоретическом расчете по методике оценки разборчивости речи, и показывают, что потенциально данный эффект может приводить к существенным отклонениям в результатах. В дальнейшем планируется провести серию артикуляционных испытаний [9, 10] для подтверждения влияния ОК на результаты оценки.

Литература

1. Покровский Н. Б. Расчет и измерение разборчивости речи. М.: Связьиздат, 1962. 390 с.
2. Железняк В. К. Некоторые методические подходы к оценке эффективности защиты речевой информации / В.К. Железняк, Ю.К. Макаров, А.А. Хорев // Специальная техника. 2000. № 4. С. 39–45
3. Трушин В. А. О корректировке методики оценки защищённости речевой информации от утечки по техническим каналам / В. А. Трушин, А. В. Иванов, И. Л. Рева // Специальная техника. - 2016. – № 6. – С. 22-30.

4. Дидковский В.С. Акустическая экспертиза каналов речевой коммуникации / В.С. Дидковский, М.Л. Дидковский, А.Н. Продеус. – Киев: Имекс-ЛТД, 2008. – 420 с.
5. Авдеев В.Б. Оценка словесной разборчивости речи в условиях воздействия помех. Часть 2 / Авдеев В.Б., Анищенко А.В., Петигин А.Ф., Трушин В.А. // Телекоммуникации. 2025. № 1. С. 29-35.
6. Хорев А. А. Анализ предельных возможностей методов шумопонижения и реконструкции речевых сигналов, маскируемых различными типами помех / А.А. Хорев, Дворянкин С. В., Козлачков С.Б., Василевская Н.В. // Вопросы кибербезопасности. 2024 .- № 1 (59) .- С. 89 - 100
7. Справочник проектировщика. Защита от шума / под ред. Е. А. Юдина. — М.: Стройиздат, 1974. — 134 с.
8. Иванов А.В. О спектре речевого акустического сигнала в вопросе оценки защищенности речевой информации от утечки по техническим каналам // В сборнике: Радиоэлектронные устройства и системы для инфокоммуникационных технологий ("РЭУС-ИТ 2025"). Доклады Всероссийской конференции, посвящённой «Дню радио». Москва, 2025. С. 345-350.
9. ГОСТ Р 50840–95. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. М.: ИПК Издательство стандартов, 1996. 198 с.
10. ГОСТ 16600-72. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений

ABOUT INFLUENCE OF ENCLOSING STRUCTURES ON THE SPEECH SIGNAL SPECTRUM WHEN ASSESSING INFORMATION SECURITY AGAINST LEAKAGE THROUGH THE ACOUSTIC CHANNEL

Associate Professor, Ph.D. A.V. Ivanov, Assistant S.R. Filimonova

Novosibirsk State Technical University

This article addresses issues related to assessing the security of acoustic speech information against leakage through technical channels, specifically evaluating the influence of various frequency-dependent attenuation characteristics of enclosing structures on the averaged speech signal spectrum and on the resulting security indicator (speech intelligibility). Dependencies of speech intelligibility on the signal-to-noise ratio are constructed for the case of using white noise as a masking interference, as well as for speech signal spectra modified by the influence of enclosing structures. The following enclosing structures were considered: door, wall, and ventilation system. Measurements necessary for assessing speech intelligibility were carried out. The results demonstrate the necessity of accounting for the frequency characteristics of sound insulation of enclosing structures when assessing the protection of premises against leakage of speech acoustic information through technical channels.



О ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ КОМБИНАЦИИ ПОЛИТИК БЕЗОПАСНОСТИ СРЕДСТВАМИ WINDOWS ACTIVE DIRECTORY DOMAIN SERVICES

студ. Кальченко М.Д.

Национальный исследовательский университет «МИЭТ»

В данной работе рассматривается возможность реализации и комбинирования различных моделей управления доступом средствами Windows Active Directory Domain Services. Анализируются дискреционная, ролевая, атрибутивная и мандатная модели доступа, а также соответствующие им технологические механизмы операционной системы Windows и AD DS: дескрипторы безопасности, списки контроля доступа, группы безопасности, организационные единицы, делегирование полномочий и т.д. Показано, что указанные модели поддерживаются платформой Microsoft в разной степени. Дискреционная модель является базовой для системы на основе ОС Windows. Ролевая реализуется через группы безопасности и делегирование полномочий. Атрибутивная модель доступа задается через механизмы Dynamic Access Control. А мандатная представлена только отдельными элементами на уровне операционной системы. Сделан вывод о целесообразности построения гибридной политики безопасности, в которой различные модели доступа не заменяют друг друга, а формируют взаимодополняющие уровни разграничения доступа в доменной инфраструктуре.

Среди основных сервисов обеспечения безопасности в вычислительных сетях и системах в соответствии с [1] аутентификация (установление идентичности и аутентичности субъектов разного типа), неотказуемость (проверка и доказательство идентичности субъекта), контроль и обеспечение целостности (как сохранение и проверка аутентичности объектов), обеспечение конфиденциальности (изоляция и защита от НСД) и управление доступом (защита от НСД). Несмотря на то что последние два их перечисленных сервисов схожи по смыслу, но могут отличаться, но как правило направлены на разные сферы. В одном случае защита ориентирована, прежде всего, на отражение внешних угроз, а во втором на «внутренние» угрозы, на которые совместно с несанкционированным внедрением вредоносных программ приходится более 70% известных нарушений информационной безопасности [2].

В настоящее время для реализации управления доступом используются подходы на основе моделей DAC (дискреционное управление доступом), MAC (мандатное управление доступом), RBAC (ролевое управление доступом) и ABAC (атрибутивное управление доступом)[3]. При этом основными считаются модели ролевого и атрибутивного доступа [4]. Если не рассматривать детально достоинства и недостатки различных моделей важно отметить, что модели дискреционного и мандатного доступа были исследованы на доказательство свойств их корректности и кроме того для государственных и военных систем наличие мандатного подхода, использующего уровни конфиденциальности, для управления потоками информации является обязательным [5]. В частности в защищенных версиях программного обеспечения Astra Linux и Postgres используется комбинация дискреционного и потокового управления: ДП-модель [6]. В тоже время ролевое и атрибутивное управление позволяют значительно упростить распределение полномочий доступа, упростить их изменение и контроль. Все эти модели в той или иной степени можно использовать в протоколе LDAP (Lightweight Directory Access Protocol) [7], который составляет основу управления доступом для сетевых продуктов Windows Active Directory [8].

При применении той или иной модели доступа к доменной инфраструктуре важно понимать, что их реализация осуществляется технологиями не только Active Directory Domain Service (AD DS), но и механизмами безопасности самой операционной системы Windows. Так сама служба каталогов AD DS предоставляет логическую структуру каталога, содержащую в себе домены, организационные единицы (organizational units - OU) и объекты, а также может поддерживать централизованное администрирование и наследование прав. В то же время принятие решения о предоставлении доступа остается за Windows посредством общей архитектуры безопасности: через дескрипторы безопасности, права, наследование, маркеры доступа, пользовательские привилегии и аудит.

Дискреционная модель доступа является базовой для операционной системы Windows и AD DS. Её сущность заключается в том, что доступ к объекту определяется набором разрешений, связанных с этим объектом, а также субъектами которым такие разрешения предоставлены или запрещены. В Active Directory каждый объект каталога обладает собственным дескриптором безопасности, который может содержать дискреционный список управление доступом (discretionary access control list - DACL). DACL, в свою очередь, состоит из записей управления доступом (access control entries - ACE), каждая из которых разрешает или запрещает определенный набор операций конкретному пользователю или группе. Для объектов каталога такими операциями могут выступать чтение и изменение содержимого, создание дочерних объектов, удаление объектов, изменение разрешений и другие действия.

Технологически дискреционная модель в Windows и AD DS реализуется через дескрипторы безопасности, списки DACL, записи ACE, идентификаторы безопасности SID и маркеры доступа access token, включающий SID самого субъекта и SID всех групп, членом которых он является. При обращении к

объекту выполняется сопоставление содержимого access token с ACE в DACL объекта, в результате чего принимается решение о предоставлении или запрете доступа. Таким образом, дискреционная модель доступа в Active Directory реализуется как классическая объектно-ориентированная схема управления доступов на основе списков доступа.[9]

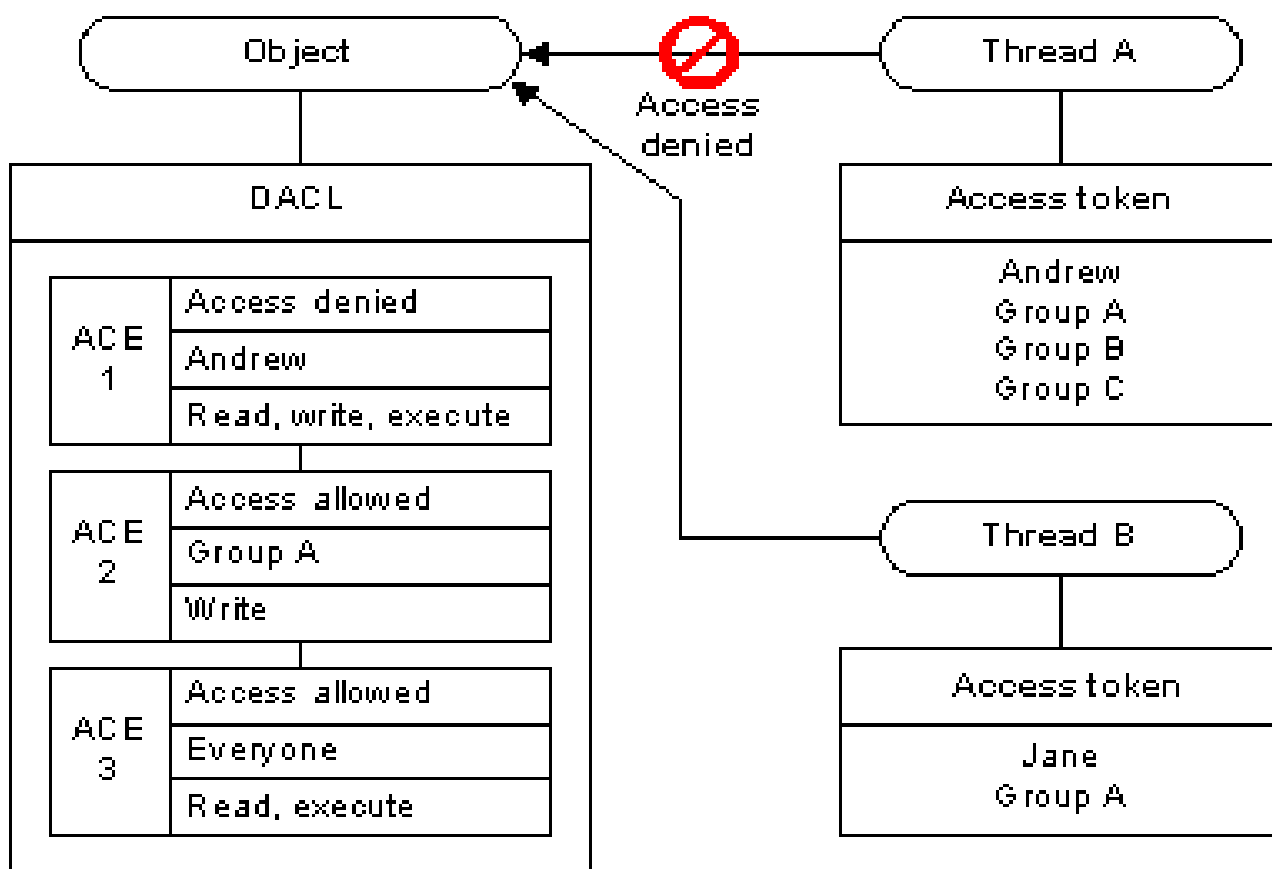


Рисунок 1. Пример принятия решения при дискреционном разграничении доступа

Ролевая модель доступа в AD DS не представлена в виде отдельного специализированного RBAC-модуля, однако практически реализуется средствами групп безопасности (security groups) и механизмами делегирования административных полномочий. Microsoft определяет security groups как средство объединения учетных записей пользователей, компьютеров и других групп в управляемые единицы, что позволяет назначать права не отдельным субъектам, а целым наборам субъектов. Такой подход соответствует основной идее ролевой модели доступа, при которой полномочия связываются не с конкретным пользователем, а с некоторой ролью, представленной в инфраструктуре группой безопасности.

Роль в AD DS реализуется через одну или несколько security groups, а набор полномочий роли задается правами, делегированными этим группам на организационные единицы, контейнеры, объекты каталога и сетевые ресурсы. Существенную роль играет вложенность групп, позволяющая строить иерархии ролей и наследование полномочий. Дополнительным средством выступает Delegation of Control Wizard, с помощью которого административные функции могут быть распределены между различными ролями без предоставления избыточных привилегий на весь домен. Следовательно, ролевая модель доступа в Active Directory реализуется через сочетание security groups, вложенности этих групп, организационной структуры каталога и механизмов делегирования управления.

Существенную роль в практической реализации ролевой модели в Active Directory Domain Services играет организационная структура каталога, представленная прежде всего иерархией организационных единиц. OU используются для группировки объектов домена в административных целях, включая делегирования полномочий и применение политик, а контроль OU и находящимся в ней объектами определяется ACL. В этой связи OU целесообразно рассматривать как механизм задания области действия роли: если группа безопасности определяет состав субъектов, выполняющих роль, то OU определяет

множество объектов каталога, в пределах которого соответствующие полномочия реализуется. За счет делегирования управления на уровне OU и поддеревьев OU становится возможным распределение административных функций между различными группами без предоставления избыточных прав на весь домен. Таким образом, в AD DS ролевая модель практически реализуется не только через группы безопасности, но и через связку «security group – OU – делегированное право», в которой группа задает носителя роли, а организационная единица – административную границу ее применения.[9]

Атрибутивная модель доступа ориентирована на принятие решения не только по идентичности пользователя или его членству в группе, но и по совокупности атрибутов субъекта, объекта и среды выполнения. ABAC в базовой форме опирается на оценку атрибутов субъекта, атрибутов объекта, условий среды и правил, определяющих допустимую операцию [10]. Такой подход особенно важен там, где статический ролевой набор оказывается недостаточным и попытка учесть множество контекстов приводит к «взрыву ролей».

Технологическая реализация атрибутивной модели включает user claims, device claims, resource properties, file classification, Central Access Rules и Central Access Policies. Central Access Policies содержит условные выражения, использующие группы пользователей, claims пользователей, claims устройства и свойства ресурсов. Сами эти политики создаются и размещаются в Active Directory, что обеспечивает их централизованное хранение и распространение. Поэтому в контексте Windows атрибутивная модель может рассматриваться как реализуемая на базе AD DS совместно с Dynamic Access Control, особенно применительно к файловым ресурсам и централизованным правилам авторизации.[11]

Мандатная модель доступа в строгом классическом понимании не является штатной моделью доступа для AD DS. Наиболее близким к ней механизмом в Windows выступает Mandatory Integrity Control. Данный механизм вводит дополнительный уровень проверки доступа, основанный на уровнях целостности субъектов и объектов. Microsoft пишет, что метка целостности объекта хранится в его дескрипторе безопасности в виде специальной mandatory label ACE, а решение о доступе учитывает соотношение уровня целостности субъекта и объекта. При этом механизм Mandatory Integrity Control работает дополнительно к дискреционному контролю доступа, а не заменяет его.[12]

Из этого следует, что мандатная модель доступа в Windows реализована лишь частично и прежде всего на уровне операционной системы. Для AD DS как службы каталога корректнее говорить не о полной нативной реализации мандатной модели доступа, а о наличии отдельных мандатных элементов и о возможности частичного приближения к мандатному управлению за счет сочетания классификации ресурсов, централизованных правил доступа и дополнительных ограничений Windows. Иными словами, если дискреционная и ролевая модели для AD DS являются естественными и штатными, то мандатная модель в доменной инфраструктуре Microsoft требует дополнительных настроек и не представлена в виде самостоятельного полнофункционального механизма каталога.

Практический анализ показывает, что в доменной инфраструктуре Windows целесообразно говорить не о выборе одной «чистой» модели, а о построении гибридной политики. На нижнем уровне фактическое применение разрешений осуществляется средствами дискреционного контроля, поскольку именно ACL и ACE участвуют в непосредственной проверке доступа к объектам. Поверх этого уровня ролевая модель упрощает администрирование: права связываются с группами безопасности и делегированными зонами ответственности, а не с каждым пользователем по отдельности.

Атрибутивный слой позволяет дополнить ролевую схему контекстно-зависимыми ограничениями. Это особенно важно там, где одной только ролевой принадлежности недостаточно: например, когда доступ к ресурсу должен зависеть не только от роли сотрудника, но и от типа устройства, местоположения, категории данных или способа аутентификации. В таком случае RBAC обеспечивает устойчивый административный каркас, а ABAC уточняет условия допуска на основе атрибутов. Подобное комбинирование позволяет снизить число узкоспециализированных ролей и одновременно сохранить централизованную управляемость.

Мандатные элементы в данной гибридной схеме играют вспомогательную роль. Mandatory Integrity Control создает дополнительный уровень принудительной изоляции, препятствующий ряду операций даже при наличии разрешающей записи в DACL. Это не превращает AD DS в полноценную решеточную систему управления информационными потоками, однако позволяет усилить базовую авторизацию и ввести отдельные недискреционные ограничения на уровне Windows. Для систем с повышенными требованиями к безопасности такой подход может использоваться как промежуточное решение, дополняющее дискреционные и ролевые механизмы.

В результате наиболее реалистичной для Windows/AD DS является следующая схема: дискреционная модель образует базовый уровень авторизации, ролевая модель — уровень административной абстракции, атрибутивная модель — уровень контекстных ограничений, а мандатные механизмы — дополнительный уровень системной изоляции. Такое сочетание не устраняет принципиальные ограничения платформы, но

делает возможным построение гибридной политики безопасности, адаптированной к реальным задачам централизованной доменной инфраструктуры.

Проведенный анализ показал, что технологии Windows и Active Directory Domain Services поддерживают разные модели разграничения доступа не в одинаковой степени. Для AD DS естественной и штатной основой выступает дискреционная модель, реализуемая через дескрипторы безопасности, DACL, ACE, SID и access token. Ролевая модель практически реализуется за счет групп безопасности, их вложенности, организационных единиц и делегирования административных полномочий. Атрибутивная модель представлена через Dynamic Access Control и связанные с ним механизмы claims, resource properties и central access policies. Мандатный подход, напротив, выражен лишь частично — преимущественно через Mandatory Integrity Control на уровне Windows, а не как самостоятельная политика AD DS.

Следовательно, доменная инфраструктура Microsoft в наибольшей степени пригодна для построения гибридных схем доступа, в которых дискреционные механизмы обеспечивают фактическое применение разрешений, ролевая модель упрощает назначение и аудит полномочий, атрибутивный подход добавляет контекст, а мандатные элементы усиливают системную изоляцию. Такой вывод важен не только для проектирования доменной инфраструктуры, но и для разработки методик аудита, поскольку проверке должны подлежать не отдельные ACL или группы сами по себе, а корректность их совместной настройки в рамках единой политики безопасности.

Литература

1. ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. — Текст : электронный // Росстандарт : [сайт]. — URL: <https://protect.gost.ru/document.aspx?control=7&id=131456> (дата обращения: 20.04.2026).
2. Кибератаки на российские компании в 2025 году.. — Текст : электронный // SOLAR : [сайт]. — URL: <https://rt-solar.ru/analytics/reports/6432/> (дата обращения: 20.04.2026).
3. Dubey, SH A review of cloud service security with various access control methods. / SH Dubey, P. K. Rai. — Текст : непосредственный // International journal of computer science and mobile computing. — 2021. — № 10. — С. 39-45.
4. Atlam, H. F. Enhancing healthcare security: a unified RBAC and ABAC risc-aware access control approach / H. F. Atlam, Y. Yang. — Текст : непосредственный // Future internet. — 2025. — № 17. — С. 262.
5. Грушо, А. А. Теоретические основы компьютерной безопасности. / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. —, 2009. — Текст : непосредственный.
6. Шумилин, А. В. Основные элементы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в СУБД PostgreSQL, ОС специального назначения Astra Linux Special Edition / А. В. Шумилин. — Текст : непосредственный // Прикладная дискретная математика. — 2013. — № 3 (21). — С. 52-67.
7. Lightweight Directory Access Protocol (LDAP): The Protocol. — Текст : электронный // RFC : [сайт]. — URL: <https://www.rfc-editor.org/rfc/rfc4511> (дата обращения: 21.04.2026).
8. Общие сведения о доменных службах Active Directory. — Текст : электронный // Microsoft Learn : [сайт]. — URL: <https://learn.microsoft.com/ru-ru/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> (дата обращения: 21.04.2026).
9. Interaction Between Threads and Securable Objects. — Текст : электронный // Microsoft Learn : [сайт]. — URL: <https://learn.microsoft.com/en-us/windows/win32/secauthz/interaction-between-threads-and-securable-objects> (дата обращения: 21.04.2026).
10. Implementing Least-Privilege Administrative Models. — Текст : электронный // Microsoft Learn : [сайт]. — URL: <https://learn.microsoft.com/en-us/windows/win32/secauthz/interaction-between-threads-and-securable-objects> (дата обращения: 21.04.2026).
11. Dynamic Access Control Overview. — Текст : электронный // Microsoft Learn : [сайт]. — URL: <https://learn.microsoft.com/en-us/windows-server/identity/solution-guides/dynamic-access-control-overview> (дата обращения: 21.04.2026).
12. Mandatory Integrity Control mechanism. — Текст : электронный // Microsoft Learn : [сайт]. — URL: <https://learn.microsoft.com/en-us/windows/win32/secauthz/mandatory-integrity-control> (дата обращения: 21.04.2026).

ON THE POSSIBILITY OF IMPLEMENTING A COMBINATION OF SECURITY POLICIES USING WINDOWS ACTIVE DIRECTORY DOMAIN SERVICES

student M. D. Kalchenko

National Research University of Electronic Technology

This work examines the possibility of implementing and combining different access control models by means of Windows Active Directory Domain Services. The study analyzes discretionary, role-based, attribute-based and mandatory access control models, as well as the corresponding Windows and AD DS mechanisms, including security descriptors, access control lists, security groups, organizational units, delegation of control etc. This research shows that these models are supported by the Microsoft platform to different degrees. The discretionary model forms the basic access control mechanism. The role-based model is implemented through security groups and delegation. The attribute-based model is supported through Dynamic Access Control. While the mandatory model is represented only by separate operating-system-level mechanisms. The article concludes that a hybrid security policy is the most practical approach for Windows domain infrastructures, where different access control models do not replace each other but form complementary layers of authorization and security enforcement.



ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПЕРЕХВАТА ТЕКСТОВОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ БЕСПРОВОДНОЙ КЛАВИАТУРЫ

студ. Карасев Н.А.

Национальный исследовательский университет «МИЭТ»

Проведён анализ протокола передачи данных беспроводной клавиатуры Microsoft Wireless Keyboard 800, работающей в диапазоне 2,4 ГГц, и выявлены его системные уязвимости: использование XOR-шифрования с MAC-адресом приёмника в качестве ключа, передача которого осуществляется в открытом виде. На основании результатов анализа разработан программно-аппаратный комплекс перехвата на базе микроконтроллера Arduino Nano и радиомодуля nRF24L01+. В ходе практических испытаний комплекс обеспечил восстановление вводимого текста в реальном времени без потерь и ошибок.

Беспроводные клавиатуры прочно вошли в повседневную практику как корпоративных пользователей, так и частных лиц. По данным аналитических агентств, к 2024 году доля беспроводных периферийных устройств среди проданных клавиатур превысила 46%. [1]. Столь значительный рост популярности беспроводных устройств делает вопрос их безопасности особенно актуальным.

В отличие от проводных аналогов, беспроводные клавиатуры передают данные о нажатиях клавиш по открытой радиосети, что принципиально расширяет поверхность атаки. Злоумышленник, находящийся в радиусе приёма сигнала, потенциально способен перехватить вводимые пользователем учётные данные, платёжные реквизиты и иную конфиденциальную информацию. Схема канала утечки информации представлена на рисунке 1.



Рисунок 1. Схема канала утечки информации, реализуемого посредством пассивного перехвата радиосигнала

Компания Microsoft на протяжении многих лет является ведущим производителем беспроводной периферии [2]. В клавиатурах она использовала собственный протокол передачи данных на частоте 2,4 ГГц, в котором нажатия клавиш шифруются операцией XOR с ключом. Передаваемый пакет имеет фиксированную структуру, состоящую из 4-ех полей (рисунок 2)

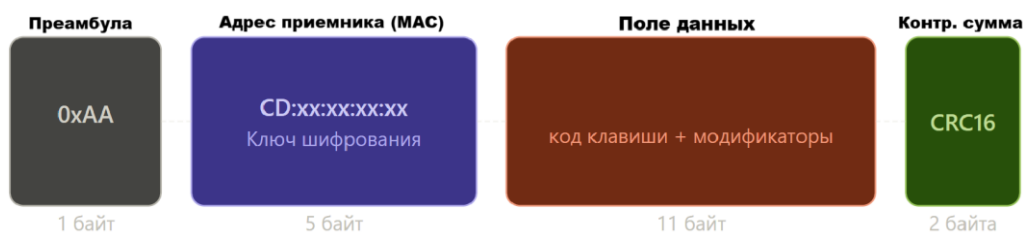


Рисунок 2. Структура пакета протокола Microsoft 2,4 ГГц

Поле препамбулы выполняет роль синхронизирующей последовательности, позволяющей приёмнику правильно определить начало пакета. Поле адреса содержит MAC-адрес USB-приемника, для принятия пакетов, которые адресованы именно ему. Поле данных содержит зашифрованную информацию о нажатой клавише. Поле контрольной суммы обеспечивает обнаружение ошибок при передаче.

На рисунке 3 приведена побайтовая иллюстрация механизма XOR-шифрования на примере нажатия клавиши «b».

Формирование пакета при нажатии клавиши "b"																
Шифр текст	0A	78	06	01	C2	98	76	0A	C0	C8	98	35	0A	C0	CD	5B
Ключ					CD	98	35	0A	C0	CD	98	35	0A	C0	CD	
Открытый текст	0A	78	06	01	0F	00	43	00	00	05	00	00	00	00	00	
	Device type	Packet type	Model	?	Sequence ID	Flags/Meta				HID Code						Checksum

Рисунок 3. Формирование пакета при нажатии клавиши «b»

В ходе анализа протокола были выявлены следующие уязвимости [3, 4, 5]:

- MAC-адрес приемника, который передается в открытом виде, является ключом для XOR-шифрования;
- шифрование применяется в режиме ECB (Electronic Code Book), т.е. нажатие клавиши «b» всегда даёт один и тот же зашифрованный байт;
- все беспроводные клавиатуры Microsoft используют MAC-адрес, начинающийся с байта 0xCD.

Поскольку нажимаемая клавиша выровнена именно с первым байтом MAC, возможно расшифровать любое нажатие, даже не зная полного MAC-адреса (рисунок 3);

- все пакеты Microsoft-клавиатур начинаются с байта 0xAA (преамбула).

Таким образом, выявленные уязвимости протокола передачи данных свидетельствуют о потенциальной возможности перехвата текстовой информации, вводимой с беспроводной клавиатуры. На основании проведённого анализа разработана структурная схема комплекса перехвата, представленная на рисунке 4.

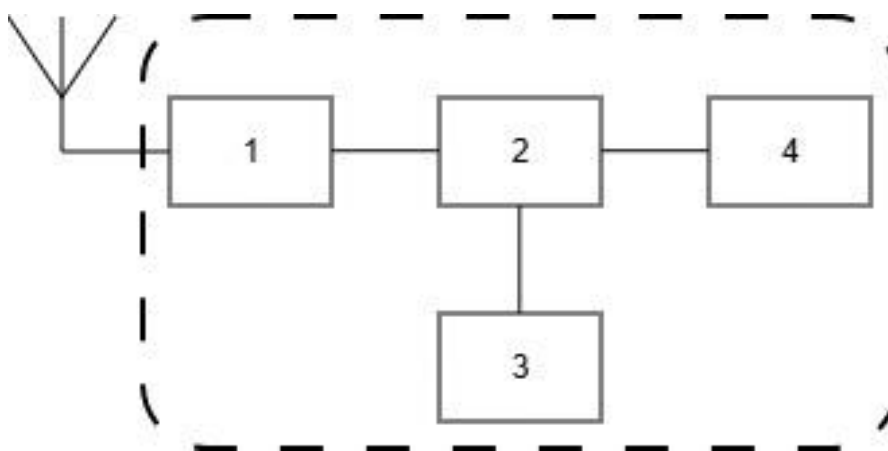


Рисунок 4. Структурная схема комплекса перехвата: 1 — приёмное устройство; 2 — микроконтроллер; 3 — источник питания; 4 — устройство хранения и отображения информации

Приёмное устройство 1 осуществляет приём радиосигналов в диапазоне работы беспроводной клавиатуры. Микроконтроллер 2 выполняет обработку принятых данных, а также расшифрование информации. Источник питания 3 обеспечивает работоспособность всех компонентов комплекса. Устройство хранения и отображения информации — предназначено для сохранения полученных данных, их последующего анализа.

На основании разработанной структурной схемы был реализован программно-аппаратный комплекс, принципиальная схема и внешний вид которого представлены на рисунках 5 и 6.

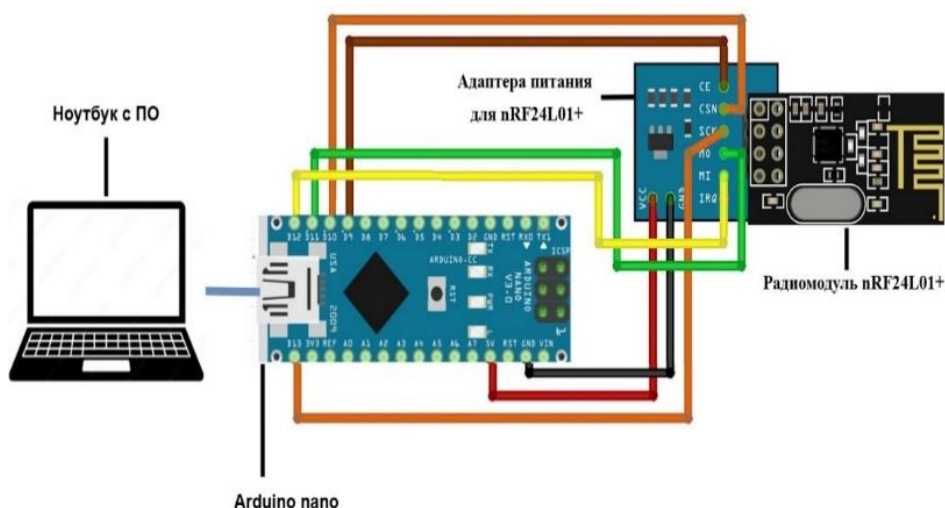


Рисунок 5. Принципиальная схема комплекса перехвата

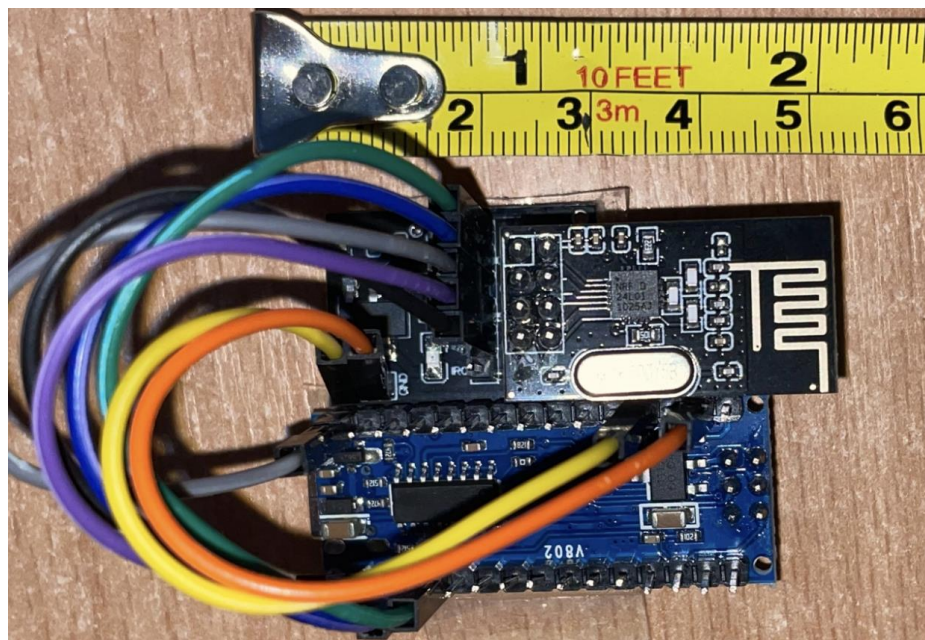


Рисунок 6. Внешний вид комплекса перехвата

Функции приёмного устройства выполняет радиомодуль «nRF24L01+», обеспечивающий работу в диапазоне 2,4 ГГц и сканирование частотных каналов. В качестве микроконтроллера используется «Arduino Nano», осуществляющий управление радиомодулем, анализ принятых пакетов и их XOR-расшифровку. Источник питания реализован с использованием адаптера питания для «nRF24L01+», обеспечивающего стабилизацию напряжения. Функции устройства хранения и отображения информации выполняет ноутбук с установленным программным обеспечением «Arduino IDE», принимающий и отображающий данные через интерфейс USB.

В среде Arduino IDE был разработан программный модуль, реализующий следующий алгоритм работы:

- настройка параметров сканирования частотного диапазона 2403-2480 МГц;
- последовательное сканирование каналов диапазона 2,4 ГГц с шагом 1 МГц в поисках пакетов с преамбулой 0xAA и первым байтом адреса 0xCD;
- при обнаружении потенциальной клавиатуры: фиксация канала и MAC-адреса приемника;
- в случае успешного обнаружения: непрерывный приём пакетов, XOR-расшифровка и вывод информации о нажатых клавишах в монитор последовательного порта.

Для подтверждения работоспособности разработанного программно-аппаратного комплекса был проведён эксперимент по перехвату данных, передаваемых беспроводной клавиатурой. В качестве объекта исследования использовалась клавиатура Microsoft Wireless Keyboard 800 Model 1455 (рисунок 7). Комплекс

перехвата размещался на удалении около 5 метров от автоматизированного рабочего места, оснащённого беспроводной клавиатурой.



Рисунок 7. Клавиатура Microsoft Wireless Keyboard 800

В ходе сканирования система обнаружила устройства с MAC-адресами, однако они не содержали характерный байт 0xCD. Далее была зафиксирована клавиатура (с MAC-адресом, соответствующим требованиям) на канале 19, после чего система приступила к приёму пакетов (рисунок 8).

```
02:40:29.383 -> Настройка радиоканала
02:40:29.383 -> Настройка завершена
02:40:29.383 -> Начало поиска
02:40:29.383 -> Поиск на 2419 МГц
02:40:30.587 -> Потенциальная клавиатура с MAC-адресом: A0 0 AA DD CD 7E 95 A1
02:40:35.293 -> Потенциальная клавиатура с MAC-адресом: A9 80 4D C8 CD 43 5 3C
02:40:35.293 -> Клавиатура найдена! Передача на канале 19
02:40:35.293 -> 2setupRadio
02:40:35.334 -> 8: 0A 38 1E 01 80 02 00 50
02:40:35.334 -> 8: 0A 38 1E 01 80 02 00 50
02:40:35.367 -> 8: 0A 38 1E 01 80 02 00 50
02:40:35.440 -> 8: 0A 38 1E 01 80 02 00 50
02:40:35.475 -> 16: 0A 78 1E 01 81 02 43 00 00 00 00 00 00 00 00 9A
```

Рисунок 8. Поиск беспроводной клавиатуры

Для подтверждения корректности приёма и расшифровки пакета на клавиатуре была нажата клавиша «b». Комплекс зафиксировал пакет, расшифровал его и также вывел «b» (рисунок 9). При этом содержимое пакета совпадает с процессом его формирования на клавиатуре, описанным на рисунке 3.

```
19:37:52.266 -> Полученный пакет: 0A 78 1E 01 59 C8 0E 80 A9 C8 C8 4D 80 A9 CD 88
19:37:52.308 -> Ключ: CD C8 4D 80 A9
19:37:52.308 -> Расшифрованный пакет: 0A 78 1E 01 94 00 43 00 00 05 00 00 00 00 00 88
19:37:52.308 -> Text: b (HID: 0x5)
```

Рисунок 9. Перехват пакета при нажатии клавиши «b»

Для итоговой оценки достоверности и полноты перехвата был эксперимент в режиме непрерывного ввода текста. На клавиатуре набиралась классическая проверочная фраза, содержащая все буквы русского алфавита: «съешь ещё этих мягких французских булок, да выпей же чаю». Комплекс перехватывал каждый пакет нажатий клавиш в реальном времени, расшифровывал и фиксировал соответствующие символы. В результате, журнал перехваченных символов отобразил исходную фразу без ошибок и пропусков (рисунок 10).


```
08:31:13.869 -> Запись перехваченного текста:  
08:33:18.927 -> съешь ещё этих мягких французских булок, да выпей же чаю.
```

Рисунок 10. Результат перехвата фразы

Таким образом, беспроводные клавиатуры даже ведущих производителей, позиционируемые как устройства с шифрованием пакетов, содержат в реализации протокола уязвимости, которые позволяют пассивному наблюдателю за радиоэфиром восстановить содержимое перехваченных пакетов. Данный вывод подтвержден как теоретически, так и практически. Использование подобных устройств создает неконтролируемый канал утечки информации, реализация которого не требует дорогостоящего оборудования, привилегированного доступа к системе или активного воздействия на радиоканал, что существенно повышает практическую опасность данной угрозы. В результате, уровень защиты беспроводных клавиатур Microsoft с XOR-шифрованием недостаточен для применения их на автоматизированных рабочих местах, обрабатывающих сведения ограниченного доступа.

Литература

1. Рынок компьютерных клавиатур [Электронный ресурс] // Data Bridge Market Research. — Режим доступа: <https://www.databridgemarketresearch.com/ru/reports/global-computer-keyboards-market> (дата обращения: 03.03.2025).
2. Компьютерные клавиатуры и мыши (мировой рынок) [Электронный ресурс] // TAdviser. — Режим доступа: [https://www.tadviser.ru/index.php/Статья:Компьютерные_клавиатуры_и_мыши_\(мировой_рынок\)](https://www.tadviser.ru/index.php/Статья:Компьютерные_клавиатуры_и_мыши_(мировой_рынок)) (дата обращения: 03.03.2025).
3. Kamkar S. KeySweeper: Covert Microsoft Wireless Keyboard Logger [Электронный ресурс] / S. Kamkar. — 2015. — Режим доступа: <https://samy.pl/keysweeper> (дата обращения: 10.04.2025).
4. Schroeder T. Practical Exploitation of Modern Wireless Devices [Электронный ресурс] / T. Schroeder, M. Moser // CanSecWest Applied Security Conference. — Vancouver, 2010. — Режим доступа: https://www.remote-exploit.org/content/keykeriki_v2_cansec_v1.1.pdf (дата обращения: 15.04.2025).
5. Newlin M. MouseJack: Injecting Keystrokes into Wireless Mice and Keyboards [Электронный ресурс] / M. Newlin. — Bastille Networks, 2016. — Режим доступа: <https://www.bastille.net/research/vulnerabilities/mousejack> (дата обращения: 15.04.2025).

INVESTIGATION OF THE POSSIBILITY OF INTERCEPTING TEXT INFORMATION USING A WIRELESS KEYBOARD

Stud. Karasev N.A.

National Research University of Electronic Technology

The analysis of the Microsoft Wireless Keyboard 800 wireless keyboard protocol operating in the 2.4 GHz data transmission range has been carried out, and its system vulnerabilities have been identified: the use of XOR encryption with the receiver's MAC address as a key, which is transmitted in clear text. Based on the analysis results, an interception software and hardware complex based on the Arduino Nano microcontroller and the nRF24L01+ radio module has been developed. During practical tests, the complex provided real-time recovery of the entered text without loss and errors.



ОБЗОР УГРОЗ УПРАВЛЯЮЩИМ СИГНАЛАМ БПЛА

студ. Кононов В.О.

Национальный исследовательский университет «МИЭТ»

В статье рассматриваются основные угрозы управляющим сигналам беспилотных летательных аппаратов и показывается, что уязвимость радиоканала управления является ключевым фактором риска для безопасной эксплуатации БПЛА. Проанализированы перехват и расшифрование трафика, имитация и модификация команд, replay-атаки, синхронная подмена, а также глушение управляющих сигналов и воздействие на навигацию средствами GPS-джемминга и GPS-спуфинга. Особое внимание уделено механизмам реализации этих атак и их возможным последствиям, включая перехват управления, искажение телеметрии, срыв миссии и аварийные режимы полёта. Сделан вывод о необходимости комплексной защиты протоколов обмена, аутентификации команд, контроля целостности и свежести сообщений, а также повышения помехоустойчивости каналов связи и навигации.

[3] Система управления БПЛА как объект воздействия

Прежде чем переходить к классификации угроз, необходимо кратко обозначить, каким образом организовано управление беспилотным аппаратом. С практической точки зрения канал управления обычно включает два направления обмена. Первое направление — от оператора к БПЛА — содержит командную информацию. Именно здесь передаются значения каналов газа, крена, тангажа и рыскания, а также команды изменения режима, возврата домой, запуска миссии, посадки и так далее. Второе направление — от БПЛА к оператору — передает телеметрию: координаты, скорость, состояние батареи, ориентацию, сигналы полезной нагрузки. Для безопасности оба направления одинаково важны. Командный канал определяет, что аппарат будет делать, а телеметрический — что оператор будет о нем знать.

Особенность большинства современных БПЛА состоит в том, что эти данные передаются в ограниченном по мощности и ширине полосы радиоканале, для которого приоритетами часто становятся дальность, задержка и устойчивость к помехам. На практике это нередко приводит к тому, что вопросы аутентификации команд и защиты от повторной отправки оказываются реализованными неполноценно, а иногда и вовсе игнорируются. Именно отсюда вытекают многие угрозы, которые на первый взгляд могут казаться разрозненными, но фактически имеют общий корень: недостаточную защищенность протокола обмена.

[4] Перехват трафика как базовая предпосылка различных угроз

Перехват управляющих сигналов — это не просто одна из угроз наряду с другими, а фундаментальный этап, на котором строится значительная часть последующих атак. Чтобы изменить пакет, повторно его отправить, воспроизвести командную последовательность или изучить структуру протокола, злоумышленник должен сначала получить доступ к самому сигналу. По этой причине анализ угроз каналу управления целесообразно начинать именно с перехвата.

В простейшем случае речь идет о пассивном радионаблюдении. Нарушитель не излучает ничего в эфир, а лишь принимает и записывает сигнал. Это делает подобную атаку особенно опасной: факт перехвата трудно обнаружить, а для оператора и самого БПЛА канал продолжает выглядеть так же, как и выглядел до этого. Если протокол не использует шифрование, злоумышленник получает содержимое пакетов в явном виде или, по крайней мере, после сравнительно несложного декодирования. В этом случае становятся известны команды управления, структура кадров, идентификаторы устройств, формат телеметрии и характер служебных полей.

Даже если содержимое пакета не сразу поддается интерпретации, сам по себе факт захвата пакета уже представляет определённую ценность. По временной структуре, длительности пакетов, используемым частотам и повторяющимся полям можно восстановить логику протокола, определить интервалы обмена, выделить постоянные и переменные части сообщения. В ряде случаев этого достаточно, чтобы перейти к построению собственного передатчика, способного имитировать легитимный источник.

[5] Расшифрование и аналитическая обработка перехваченного трафика

Перехват сигнала сам по себе еще не означает понимания его содержания. Однако если канал не шифруется либо использует слабую или неправильно реализованную схему защиты, следующий шаг нарушителя — аналитическая обработка трафика и попытка восстановления сути передаваемых данных. На этом этапе атака переходит из радиоэлектронной в криптографическую плоскость.

Если протокол передает данные в открытом виде, задача практически сводится к выделению структуры сообщения. Например, можно быстро установить, какие поля изменяются при отклонении стика газа, какие — при изменении курса, какие служат идентификаторами или счетчиками.

Сложнее обстоит дело, если в канале связи используется шифрование. Однако и здесь у злоумышленника остаются варианты. Во-первых, применяемый алгоритм может быть устаревшим или выбранным без учета угрозы модификации данных. Во-вторых, возможны ошибки в управлении ключами, инициализирующими векторами и режимами работы. В-третьих, нередко на практике встречается ситуация, при которой шифруется только часть полезной нагрузки, а управляющие или служебные поля остаются в открытом виде.

Не менее важен и вопрос извлечения закономерностей без полного расшифрования. Иногда достаточно знать, что определенный тип пакета отправляется непосредственно перед посадкой, активацией возврата домой или переходом в режим зависания. Тогда атакующий может не читать содержание каждого байта, а использовать сам факт появления определенной последовательности.

[6] Имитация команд и внедрение ложных пакетов

Одной из наиболее опасных угроз для управляющих сигналов является их имитация, то есть формирование нарушителем пакета, внешне похожего на легитимное сообщение от оператора. Эта атака может строиться на разных уровнях сложности. В самом простом варианте злоумышленник лишь копирует формат пакета и подбирает значения полей, рассчитывая на отсутствие у приемника строгой проверки источника. В более сложном варианте он предварительно изучает структуру протокола, идентификаторы устройств, механизм синхронизации и дополнительные служебные параметры, после чего создает сообщения, которые система воспринимает как штатные.

Опасность имитации состоит в том, что она открывает путь к фактическому навязыванию БПЛА чужой воли. Если аппарат принимает ложный пакет за подлинный, последствия могут быть самыми разными: от незначительного отклонения курса до полного перехвата управления, аварийной посадки или ухода в заранее заданную точку. В отличие от простого глушения, которое лишь прерывает управление, имитация сохраняет внешнюю работоспособность канала. С точки зрения оператора это значительно опаснее, поскольку аппарат продолжает реагировать на команды, но уже не на те, которые были отправлены законным пользователем.

[7] Модификация сообщений и инверсия битов

Рассматривая угрозы управляющим сигналам, нельзя ограничиваться только чтением или полной подделкой пакетов. На практике существует промежуточный, но крайне опасный класс атак, связанных с модификацией уже передаваемого сообщения. В этом случае злоумышленник не создает пакет с нуля, а вносит изменения в легитимный трафик, рассчитывая на то, что приемник не обнаружит вмешательство.

В наиболее общем виде такая атака может заключаться в изменении отдельных полей кадра: например, параметра высоты, угла поворота, скорости, режима полета. Даже малое вмешательство способно привести к существенным последствиям. Для беспилотного аппарата команда с немного измененным значением может оказаться не менее опасной, чем полностью ложная команда, особенно если она поступила в ответственный момент маневра.

Особое место здесь занимает так называемая атака инверсии битов. Она особенно характерна для тех случаев, когда разработчик применяет шифрование без полноценного контроля целостности. При определенных режимах работы злоумышленник способен изменить отдельные биты шифртекста так, что после расшифрования на стороне приемника возникнут предсказуемые искажения открытого текста. Иными словами, нарушитель может не знать точного содержания команды, но все равно воздействовать на нее осмысленным образом.

Для БПЛА такая возможность крайне опасна. Если структура пакета известна, достаточно понимать, какие байты отвечают за конкретные параметры. Тогда вмешательство в шифртекст может изменить, например, значение газа, параметр курса или флаг режима полета. Даже если результат будет не абсолютно точным, вероятность возникновения критической ситуации остается высокой.

[8] Повторное использование перехваченных сигналов

Повторная отправка перехваченных управляющих пакетов, или replay-атака, по праву считается одной из наиболее характерных угроз для беспроводных систем управления. Ее опасность заключается в том, что нарушителю не требуется понимать содержание сообщения или уметь формировать новый корректный пакет. Достаточно один раз записать легитимную команду, а затем воспроизвести ее в другой момент времени.

На первый взгляд может показаться, что такая атака менее опасна, чем полноценная имитация. Однако для БПЛА это далеко не так. Многие команды имеют критическое значение независимо от контекста: активация возврата домой, запуск заданного режима, аварийная остановка, изменение маршрута, команда на

снижение или разворот. Если такая команда будет повторно введена в эфир в неподходящий момент, аппарат может выполнить действие, которое уже не соответствует текущей ситуации полета.

Replay-атака особенно коварна тем, что повторно передаваемый пакет действительно когда-то был легитимным. Следовательно, если протокол не умеет отличать старое допустимое сообщение от нового допустимого сообщения, формальных оснований для отклонения пакета у приемника нет. Именно в этом состоит принципиальная слабость многих простых схем защиты. Шифрование без контроля свежести данных не решает проблему: старый зашифрованный пакет остается корректным зашифрованным пакетом.

[9] Атаки синхронной подмены и временные атаки

Ещё одной атакой, которая хоть по сути своей и включает в себя такие атаки как подмена, имитация, повторная отправка, является атака синхронной подмены или атака по времени. Поскольку мы рассмотрели уже пути работы злоумышленника с самими пакетами, то здесь мы ограничимся рассмотрением самого механизма атаки.

В рамках данной атаки речь идет о случаях, когда нарушитель не просто передает ложное сообщение в произвольный момент, а стремится встроиться во временную структуру легитимного обмена: отправить пакет чуть раньше, одновременно или в строго рассчитанное окно между штатными кадрами.

Причины эффективности такого подхода понятны. Во многих радиосистемах приемник ориентируется не только на содержание пакета, но и на временную организацию канала. Если злоумышленнику удастся подать свой сигнал в момент, когда приемник ожидает очередной кадр, вероятность успешного приема возрастает. Особенно это актуально для систем с перестройкой рабочей частоты, слотированной передачей или жестким ритмом обмена.

С практической точки зрения временная атака может использоваться в двух основных вариантах. В первом варианте вредоносный пакет подается чуть раньше легитимного и перехватывает внимание приемника. Во втором — он передается синхронно, вызывая коллизию и создавая условия, при которых законный кадр не будет принят, а последующая логика системы перейдет в аварийный или деградированный режим.

[10] Глушение управляющего сигнала

Глушение, или jamming, относится к числу наиболее известных и наглядных способов противодействия БПЛА. Суть его состоит в создании в зоне работы приемника такого уровня помех, при котором полезный сигнал оператора перестает адекватно приниматься. На физическом уровне это означает снижение отношения сигнал/шум до значений, при которых корректное восприятие пакетов становится невозможным.

Большинство систем радиоэлектронного подавления БПЛА состоит из двух условных подсистем — система обнаружения и система подавления.

Рассмотрим системы обнаружения. Их задача — установить местонахождение БПЛА в данный момент времени и направить подсистему радиоэлектронного подавления. В боевых системах подавления они представлены радио радарами, которые ведут поиск на частотах управляющих сигналов БПЛА. Диапазон поиска обыкновенно составляет 0,5 – 5 ГГц.

Однако, существуют и альтернативные системы выявления БПЛА, например, основанные на оптическом обнаружении. В данный момент они всё больше набирают популярность в связи с развитием искусственного интеллекта и нейронных сетей, поскольку чаще всего подобный метод основан на том, что камера получает изображение неба в реальном времени, а специально натренированная модель определяет наличие и местоположение БПЛА, возможно и его направление и скорость движения.

Не является очевидным, но крайне часто подсистемой обнаружения является сам человек. Всевозможные «ружья» против БПЛА используют именно человека для поиска и направления антенн. Человек, оперирующий системой подавления самостоятельно визуально или акустически определяет местонахождение БПЛА и совершает наведение системы радиоэлектронного подавления.

И наконец, системы обнаружения может просто не быть в комплексе. Если используется ненаправленная антенна, то комплекс глушит сигнал во всех направлениях и его наводка не является необходимой.

Само радиоэлектронное подавление можно разделить на два больших вида: широкополосное и узкополосное. Принцип в обоих случаях заключается в том, чтобы вокруг БПЛА создать такой электромагнитный шум, чтобы отношение сигнал/шум на входе приёмника БПЛА было достаточно низким для того, чтобы управляющий сигнал не мог бы быть принят и обработан.

Если подавление происходит в широкополосном диапазоне частот, то он должен быть таким, чтобы перекрывать большую часть возможных частот, на которых ведётся передача управляющих сигналов БПЛА. Обычно это диапазон 0,5 – 5 ГГц.

В случае же узкополосного диапазона, нам нужно точно знать, на какой частоте происходит управление, поскольку необходимо подстроиться именно на данную частоту для помехи. Однако, в отличие от широкополосного подавления, узкополосное является более энергоэффективным.

[11] **Подмена и искажение геоданных: GPS-спуфинг и GPS-джамминг**

Большое количество БПЛА используют спутниковое отслеживание расположения для тех или иных целей. Особенно актуально использование таких систем для БПЛА большой дальности. Чаще всего используются системы GPS или Глонасс. В связи с большей распространённостью GPS, то и большинство известных атак проводились именно на GPS. Тем не менее, из-за схожести принципов работы обеих систем, атаки на GPS не теряют актуальности и для системы Глонасс.

GPS-джамминг в сути своей есть просто глушение сигнала GPS, что не позволяет БПЛА определить своё местоположение. Это довольно простой процесс, который осуществляется при помощи специальных устройств, которые создают электромагнитный шум в диапазоне частот работы трекеров слежения (1100 – 1600 МГц).

GPS-спуфинг есть атака более интересная, поскольку в её ходе сигнал GPS не глушится, но подменяется совершенно иным. В итоге системы навигации продолжают функционировать, но подают совершенно неверные данные в систему. GPS-спуфинг основывается на том, что система жертвы начнёт воспринимать изначально правильный, но более мощный сигнал злоумышленника, который со временем начнёт уводить показания GPS всё дальше от верного местоположения. Но для этого нужно точно знать, где находится цель, чтобы правильно рассчитать время от атакующего до цели, поскольку, именно основываясь на нём определяется местоположение жертвы в пространстве.

В данный момент проблема атак на системы GPS и Глонасс особенно актуальна, поскольку в связи с ведением боевых действий в современных условиях с применением передового оборудования в области БПЛА, самым грубым и очевидным способом борьбы становится глушение GPS. Однако это является проблемой в т.ч. и для гражданской авиации, поскольку глушение при помощи комплексов вооружённых сил может действовать и за сотни километров от поля боя. GPS-спуфинг хоть и более сложен в исполнении, но также набирает популярность, что повышает его актуальность в качестве угрозы.

Литература

1. Аджухонов, Э. А. Комплекс перехвата управления БПЛА / Э. А. Аджухонов, О. В. Николаев // Вестник Концерна ВКО «Алмаз — Антей». — 2021. — № 2.
2. Аменитский, М. В. Анализ потенциальных угроз системы управления беспилотных летательных аппаратов средних и тяжелых классов / М. В. Аменитский // Труды МАИ. — 2017. — № 94. — URL: <https://trudymai.ru/published.php?ID=81066> (дата обращения: 12.04.2026).
3. Макаренко, С. И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Ч. 3. Радиоэлектронное подавление систем навигации и радиосвязи / С. И. Макаренко // Системы управления, связи и безопасности. — 2020. — № 2. — DOI: 10.24411/2410-9916-2020-10304. — URL: <https://sccs.intelgr.com/archive/2020-03/04-Makarenko.pdf> (дата обращения: 12.04.2026).
4. Белов, Н. В. Разработка алгоритма перехвата управления квадрокоптером Syma X8C / Н. В. Белов, Б. Я. Буянов // Студенческий научный форум — 2019 : материалы XI Международной студенческой научной конференции. — Электрон. дан. — URL: <https://scienceforum.ru/2019/article/2018013880> (дата обращения: 12.04.2026).

OVERVIEW OF THREATS TO UAV CONTROL SIGNALS

stud. Kononov V.O.

National Research University of Electronic Technology

The article examines the main threats to the control signals of unmanned aerial vehicles and shows that the vulnerability of the radio control channel is a key risk factor for the safe operation of UAVs. It analyzes the interception and decryption of traffic, command spoofing and modification, replay attacks, synchronized spoofing, as well as jamming of control signals and attacks on navigation through GPS jamming and GPS spoofing. Particular attention is paid to the mechanisms by which these attacks are carried out and to their possible consequences, including hijacking control, telemetry distortion, mission failure, and emergency flight modes. The paper concludes that comprehensive protection is needed for communication protocols, command authentication, message integrity and freshness control, as well as improved resilience of communication and navigation channels to interference.



О РАЗРАБОТКЕ МЕТОДИКИ ОЦЕНКИ АУДИТОРСКОГО РИСКА ПРИ АУДИТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

магистрант Кочедыков С.С.

Национальный исследовательский университет «МИЭТ»

В статье рассматривается задача разработки методики оценки аудиторского риска при аудите информационной безопасности субъектов критической информационной инфраструктуры. Показано, что классическая модель аудиторского риска, основанная на присущем риске, риске средств контроля и риске пропуска существенного несоответствия, требует уточнения применительно к значимым объектам критической информационной инфраструктуры. Предложен подход, в котором полнота реализации обязательных мер безопасности рассматривается не как независимый от регуляторного риска показатель, а как основа для его определения. Для учёта неоднородности элементов объекта критической информационной инфраструктуры введён критичностно-взвешенный риск необнаружения, связывающий итоговый аудиторский риск с составом программы аудита. Методика учитывает категорию значимости, состояние реализации обязательных мер безопасности, устойчивость выполнения критических функций и риск-ориентированный характер аудиторской выборки.

Ключевые слова: аудит информационной безопасности, аудиторский риск, аудиторское свидетельство, значимый объект КИИ, критическая информационная инфраструктура, риск-ориентированная выборка, устойчивость, ФСТЭК России.

Введение. Аудит информационной безопасности (ИБ) субъектов критической информационной инфраструктуры (КИИ) является важным инструментом оценки состояния защищённости, выявления несоответствий требованиям и обоснования управленческих решений по повышению уровня безопасности. В отличие от общего аудита информационных систем (ИС), аудит субъектов КИИ должен учитывать не только наличие организационных и технических мер защиты, но и категорию значимости объекта, критичность выполняемых функций, взаимосвязанность элементов инфраструктуры, а также способность объекта сохранять и восстанавливать функционирование при воздействиях.

Нормативную основу такой постановки образует Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности КИИ Российской Федерации» [1], устанавливающий правовые основы обеспечения безопасности КИИ.

Существенное значение имеет также методический документ ФСТЭК России от 11 ноября 2025 г. «Методика оценки показателя состояния технической защиты информации (ТЗИ) в ИС и обеспечения безопасности значимых объектов КИИ Российской Федерации» [2]. В нём задаётся подход к оценке текущего состояния защиты информации (ЗИ) и обеспечения безопасности значимых объектов КИИ, включая нормированное значение показателя и порядок его расчёта. Документ применяется, в том числе, для оценки степени соответствия текущего состояния ЗИ минимально необходимому уровню защиты от типовых актуальных угроз безопасности информации [2].

Цель статьи - предложить методический подход к оценке аудиторского риска при аудите ИБ субъектов КИИ с учётом нормативных требований, методики ФСТЭК России, риск-ориентированного отбора аудиторских свидетельств и устойчивости выполнения критических функций.

Научная новизна предлагаемого подхода заключается: во-первых, во введении в модель аудиторского риска показателей категориальной строгости и устойчивости выполнения критических функций, согласованных с нормативно-методическими документами ФСТЭК России; во-вторых, в разработке метода риск-ориентированной выборки, учитывающего дифференцированную критичность элементов КИИ; в-третьих, в установлении аналитической связи между составом программы аудита, критичностью элементов и риском пропуска существенного несоответствия.

1. Нормативно-методические основания оценки аудиторского риска. Аудит ИБ субъектов КИИ должен опираться на совокупность нормативных и методических источников. К основным из них относятся Федеральный закон № 187-ФЗ [1], методический документ ФСТЭК России по оценке показателя состояния ТЗИ значимых объектов КИИ [2], требования ФСТЭК России по обеспечению безопасности значимых объектов КИИ [3], требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования [4].

Методический документ ФСТЭК России от 11 ноября 2025 г. имеет принципиальное значение для рассматриваемой статьи, поскольку он связывает оценку текущего состояния защиты информации с минимально необходимым уровнем защиты от типовых актуальных угроз. В рамках аудита это позволяет рассматривать аудиторский риск не только как риск ошибочного заключения, но и как риск того, что аудиторская программа не выявит несоответствие состояния защиты информации минимально необходимому уровню.

С учётом данных документов аудиторский риск при аудите субъектов КИИ можно определить как вероятность формирования аудиторского заключения, не отражающего фактическое состояние обеспечения безопасности значимого объекта КИИ, степень соответствия установленным требованиям и способность объекта сохранять критические функции при типовых актуальных угрозах.

2. Ограничения классической модели аудиторского риска. В классической теории аудита широко используется модель:

$$AR = IR \cdot CR \cdot DR, \quad (1)$$

где: AR - аудиторский риск;

IR - присущий риск, отражающий вероятность наличия существенного несоответствия до учёта средств контроля;

CR - риск средств контроля, характеризующий вероятность того, что существующие средства контроля не предотвратят или не выявят несоответствие;

DR - риск пропуска, отражающий вероятность того, что аудиторские процедуры не выявят существенное несоответствие.

Данная модель применима для общего аудита, но при аудите субъектов КИИ имеет ряд ограничений.

Во-первых, она не учитывает категорию значимости объекта. Между тем для значимых объектов КИИ категория определяет уровень требований и допустимость остаточных рисков.

Во-вторых, модель не отражает соответствие состояния ЗИ минимально необходимому уровню, который задан в методике ФСТЭК России [2].

В-третьих, классическая модель не учитывает устойчивость выполнения критических функций. Для КИИ важен не только факт реализации мер защиты, но и способность объекта сохранять функционирование в условиях воздействий.

В-четвёртых, модель не учитывает неоднородность аудиторских свидетельств. В КИИ разные элементы имеют разную критичность: одни элементы непосредственно обеспечивают критические функции, другие выполняют вспомогательную роль.

В-пятых, обычная случайная выборка может не включить критически важные элементы, что увеличивает риск пропуска существенного несоответствия.

Поэтому для аудита субъектов КИИ требуется расширенная модель, согласованная с нормативными требованиями ФСТЭК России и ориентированная на оценку состояния безопасности значимого объекта.

3. Формальная модель объекта аудита КИИ. Субъект КИИ целесообразно рассматривать как инфраструктурную систему:

$$O^{CI} = (S, E, F, C, M^{real}), \quad (2)$$

где: O^{CI} - объект аудита КИИ;

$S = \{s_1, s_2, \dots, s_n\}$ - множество элементов объекта аудита: ВС, телекоммуникационные узлы, сегменты автоматизированных систем управления (АСУ), серверы, рабочие станции, СЗИ, организационные процессы;

E - множество связей между элементами;

$F = \{f_1, f_2, \dots, f_m\}$ - множество критических функций;

C - категория значимости;

M^{real} - множество реализованных организационных и технических мер безопасности.

Для связи элементов с критическими функциями введём отображение:

$$\Phi: S \rightarrow 2^F, \quad (3)$$

где: $\Phi(s_i)$ - множество критических функций, на выполнение которых влияет элемент s_i .

Если элемент s_i нарушается, то возможно изменение критических функций:

$$s_i \rightarrow \Delta F(s_i), \quad (4)$$

где: $\Delta F(s_i)$ - множество критических функций, которые могут быть нарушены, деградированы или временно недоступны вследствие нарушения элемента s_i .

Для связи объекта аудита с требованиями ФСТЭК России введём множество обязательных мер:

$$M^{reg}(C, T) = \{m_1, m_2, \dots, m_k\}, \quad (5)$$

где: M^{reg} - множество обязательных мер безопасности для объекта категории C и множества актуальных угроз T ;

C - категория значимости объекта;

T - множество актуальных угроз безопасности информации;

m_j - j -я обязательная мера безопасности;

k - количество обязательных мер безопасности.

4. Модель полноты реализации мер и устойчивости выполнения критических функций. Для оценки состояния реализации обязательных мер безопасности введём показатель:

$$P_M = \sum_{j=1}^k \eta_j q_j, \quad (6)$$

где: P_M - показатель полноты и качества реализации обязательных мер безопасности;

k - количество обязательных мер безопасности;

$q_j \in [0, 1]$ - степень выполнения j -й меры безопасности;

η_j - весовой коэффициент j -й меры безопасности, где $\sum_{j=1}^k \eta_j = 1$.

Показатель P_M не следует рассматривать как независимый от регуляторного риска. Напротив, остаточный регуляторный риск является производной величиной от неполноты реализации обязательных мер безопасности. В простейшем случае:

$$R_R = 1 - P_M, \quad (7)$$

где: R_R - остаточный регуляторный риск, обусловленный неполнотой реализации обязательных мер безопасности.

При необходимости учёта повышенной строгости для значимых объектов более высокой категории может использоваться нелинейная форма:

$$R_R = 1 - P_M^{\beta_M(C)}, \quad (8)$$

где: $\beta_M(C)$ - коэффициент строгости оценки полноты реализации обязательных мер безопасности для категории C .

Таким образом, P_M и R_R описывают одну и ту же область — нормативно-методическое соответствие, поэтому они не перемножаются в модели как независимые вероятностные события.

Показатель устойчивости выполнения критических функций зададим как:

$$U = K_s^{\omega_s} \cdot K_f^{\omega_f} \cdot K_t^{\omega_t}, \quad (9)$$

где: U - показатель устойчивости выполнения критических функций;

K_s - структурная целостность;

K_f - функциональная работоспособность;

K_t - своевременность восстановления;

$\omega_s, \omega_f, \omega_t$ - весовые коэффициенты, $\omega_s + \omega_f + \omega_t = 1$.

Показатель своевременности восстановления может быть выражен через время восстановления:

$$K_t = \exp\left(-\frac{T^{rec}}{T_0(C)}\right), \quad (10)$$

где: T^{rec} - фактическое или расчётное время восстановления критической функции;

$T_0(C)$ - допустимое время восстановления для категории значимости C .

Содержательно показатель U позволяет оценивать не только наличие мер безопасности, но и способность объекта сохранять выполнение критических функций и восстанавливаться в допустимые сроки.

5. Критично-взвешенный риск необнаружения и риск-ориентированная выборка. Аудит субъектов КИИ проводится в условиях ограничений по времени, ресурсам, доступу к технологическим сегментам, допустимым окнам обслуживания и доступности персонала. Поэтому выборочный контроль является практически неизбежным. Однако выборка должна учитывать неоднородность элементов объекта КИИ.

Для каждого элемента объекта аудита введём показатель критичности:

$$W_i = \alpha_f f_i + \alpha_d d_i + \alpha_v v_i + \alpha_a a_i + \alpha_r r_i, \quad (11)$$

где: W_i - критичность элемента s_i ;

f_i - вклад элемента в выполнение критических функций;

d_i - степень зависимости других элементов от s_i ;

v_i - уровень уязвимости;

a_i - атакуемость или экспонированность;

r_i - регуляторная значимость;

$\alpha_f, \alpha_d, \alpha_v, \alpha_a, \alpha_r$ - весовые коэффициенты факторов.

Все частные показатели нормируются в диапазоне $[0,1]$. Для весов выполняется условие $\alpha_f + \alpha_d + \alpha_v + \alpha_a + \alpha_r = 1$.

Вероятность включения элемента в аудиторскую выборку может быть определена как:

Вероятность включения элемента в аудиторскую выборку:

$$P_i = \frac{W_i}{\sum_{j \in S_h} W_j}, \quad (12)$$

где: P_i - вероятность включения элемента s_i в выборку;

S_h - страта, к которой относится элемент;

$\sum_{j \in S_h} W_j$ - суммарная критичность элементов данной страты.

Элементы, у которых $W_i \geq W^{crit}$, включаются в программу аудита обязательно.

Для устранения противоречия, при котором критичность элементов учитывается при планировании выборки, но не влияет на итоговый аудиторский риск, введём критичностно-взвешенный риск необнаружения:

$$R^D(\pi) = \frac{\sum_{i=1}^n W_i p_i (1 - \delta_i x_i)}{\sum_{i=1}^n W_i p_i}, \quad (13)$$

где: $R^D(\pi)$ - критичностно-взвешенный риск необнаружения существенных несоответствий при реализации программы аудита π ;

n - количество элементов объекта КИИ;

W_i - критичность i -го элемента;

p_i - априорная вероятность наличия существенного несоответствия в i -м элементе;

δ_i - вероятность обнаружения существенного несоответствия при проверке i -го элемента;

x_i - индикатор включения элемента s_i в программу аудита π .

Индикатор x_i определяется следующим образом:

$$x_i = \begin{cases} 1, & \text{если элемент } s_i \text{ включен в программу аудита,} \\ 0 & \text{если элемент } s_i \text{ не включен в программу аудита,} \end{cases} \quad (14)$$

Формула (13) показывает, что высокочитичные элементы, не включённые в программу аудита, сохраняют значимый вклад в риск необнаружения. Если элемент включён в программу аудита и вероятность обнаружения δ_i высока, его вклад в риск снижается. Тем самым критичность элементов влияет не только на формирование выборки, но и на итоговую оценку аудиторского риска.

6. Итоговая модель аудиторского риска и общая последовательность применения методики. С учётом введённых показателей итоговую модель целесообразно строить через интегральный индекс благоприятного аудиторского состояния:

$$B^{audit} = P_M^{\beta_M(C)} \cdot U^{\beta_U(C)} \cdot (1 - R^D(\pi))^{\beta_D(C)}, \quad (15)$$

где: B^{audit} - интегральный индекс благоприятного аудиторского состояния объекта КИИ;

P_M - показатель полноты и качества реализации обязательных мер безопасности;

U - показатель устойчивости выполнения критических функций;

$R^D(\pi)$ - критичностно-взвешенный риск необнаружения существенных несоответствий при реализации программы аудита π ;

$\beta_M(C)$ - коэффициент значимости полноты реализации обязательных мер безопасности для категории C ;

$\beta_U(C)$ - коэффициент значимости устойчивости выполнения критических функций для категории C ;

$\beta_D(C)$ - коэффициент значимости риска необнаружения для категории C .

Итоговый аудиторский риск определяется как:

$$AR^{CI(\pi)} = 1 - B^{audit\lambda(C)}, \quad (16)$$

или в раскрытом виде:

$$AR^{CI(\pi)} = 1 - \left[P_M^{\beta_M(C)} \cdot U^{\beta_U(C)} \cdot (1 - R^D(\pi))^{\beta_D(C)} \right]^{\lambda(C)}, \quad (17)$$

где: $AR^{CI(\pi)}$ - аудиторский риск при аудите информационной безопасности объекта КИИ по программе аудита π ;

$\lambda(C)$ - коэффициент категориальной строгости, зависящий от категории значимости.

В данной модели произведение не трактуется как произведение независимых вероятностных событий. Оно используется как мультипликативный индекс благоприятного аудиторского состояния. Это позволяет избежать методической ошибки, связанной с независимым перемножением взаимозависимых показателей, таких как полнота реализации мер безопасности и остаточный регуляторный риск.

Общая последовательность применения методики может быть представлена следующим образом.

Этап 1. Определение границ аудита. Устанавливаются субъект КИИ, значимые объекты, проверяемые сегменты, критические функции, документы, технические средства и организационные процессы.

Этап 2. Идентификация обязательных требований. Формируется множество обязательных мер безопасности $M^{reg}(C, T)$ с учётом категории значимости и множества актуальных угроз.

Этап 3. Оценка полноты реализации мер. Рассчитывается показатель P_M по формуле (6). При необходимости определяется остаточный регуляторный риск как производная величина по формулам (7) или (8).

Этап 4. Оценка устойчивости. Рассчитываются показатели K_s , K_f , K_t , после чего определяется показатель устойчивости U по формуле (9).

Этап 5. Расчёт критичности элементов. Для каждого элемента объекта аудита рассчитывается критичность W_i по формуле (11).

Этап 6. Формирование аудиторской выборки. Высококритичные элементы включаются в программу аудита обязательно, остальные выбираются с вероятностью, определяемой по формуле (12).

Этап 7. Расчёт критичностно-взвешенного риска необнаружения. Для сформированной программы аудита π рассчитывается $R^D(\pi)$ по формуле (13).

Этап 8. Расчёт итогового аудиторского риска. Определяется $AR^{CI(\pi)}$ по формуле (16) или (17).

Этап 9. Подготовка заключения. Заключение должно включать оценку полноты реализации обязательных мер безопасности, устойчивости выполнения критических функций, критичностно-взвешенного риска необнаружения и итогового аудиторского риска.

7. Обсуждение предлагаемого подхода. Предлагаемая методика отличается от классического подхода тем, что связывает аудиторский риск с состоянием безопасности значимого объекта критической информационной инфраструктуры. В традиционной модели аудиторский риск выражается через обобщённые вероятностные компоненты, тогда как для КИИ требуется учитывать состояние реализации обязательных мер безопасности, категорию значимости, устойчивость выполнения критических функций и неоднородность проверяемых элементов.

Введение показателя P_M позволяет связать аудиторский риск с полнотой и качеством реализации обязательных мер безопасности. При этом остаточный регуляторный риск не рассматривается как независимый показатель, а выводится из P_M . Это устраняет методическое противоречие, при котором полнота реализации мер и регуляторный риск описывали одно и то же явление, но использовались как независимые сомножители.

Введение показателя U позволяет оценивать не только формальную защищённость, но и способность объекта сохранять выполнение критических функций. Это особенно важно для субъектов критической информационной инфраструктуры, поскольку последствия нарушения безопасности могут проявляться не только в утрате информации, но и в нарушении технологических, управленческих или производственных процессов.

Использование критичности W_i позволяет формировать более обоснованную аудиторскую выборку, в которой высокочитичные элементы имеют приоритет. При этом критичность встроена не только в процедуру выбора элементов, но и в итоговую модель риска через $R^D(\pi)$. Это означает, что если высокочитичный элемент не включён в программу аудита, то его вклад в риск необнаружения сохраняется и влияет на итоговый аудиторский риск.

Таким образом, методика оценки аудиторского риска при аудите информационной безопасности субъектов КИИ должна соединять нормативную оценку состояния защиты, оценку устойчивости критических функций и риск-ориентированный выборочный контроль.

Заключение. В статье предложен уточнённый подход к разработке методики оценки аудиторского риска при аудите ИБ субъектов КИИ. Показано, что классическая модель аудиторского риска требует развития, поскольку не учитывает категорию значимости, состояние реализации обязательных мер безопасности, устойчивость выполнения критических функций и неоднородность аудиторских свидетельств.

С учётом методических документов ФСТЭК России введён показатель полноты и качества реализации обязательных мер безопасности P_M . Показано, что остаточный регуляторный риск не должен рассматриваться как независимый от P_M , поскольку оба показателя описывают состояние нормативно-методического соответствия. В связи с этим остаточный регуляторный риск определяется как производная величина от неполноты реализации обязательных мер безопасности.

Для учёта неоднородности элементов объекта КИИ введён показатель критичности W_i , отражающий вклад элемента в критические функции, зависимость других элементов, уровень уязвимости, атакуемость и регуляторную значимость. В отличие от подхода, при котором критичность используется только для формирования выборки, в настоящей статье она встроена в итоговую модель через критичностно-взвешенный риск необнаружения $R^D(\pi)$, а итоговая модель аудиторского риска представлена в выражении (17).

Предложенный подход позволяет учитывать категорию значимости, полноту реализации обязательных мер безопасности, устойчивость выполнения критических функций и качество риск-ориентированной выборки. В дальнейшем методика может быть развита за счёт детализации шкал оценки P_M , уточнения коэффициентов $\beta_M(C)$, $\beta_U(C)$, $\beta_D(C)$, а также разработки типовых матриц аудиторских свидетельств для различных категорий значимых объектов КИИ с учетом [10-11].

Литература

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Методический документ ФСТЭК России от 11.11.2025 «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
3. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
4. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
5. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks.
6. International Auditing and Assurance Standards Board. ISA 530 Audit Sampling.
7. Dushkin A.V., Kochedykov S.S., Novoseltsev V.I., Kobzistyy S.Y., Smolyakova S.D. Algorithm and Method for Recognizing Critical Situations Using Semantic Networks on Critical Information Infrastructure Facilities as a Result of Cyber Attacks // 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIconRus). 2020. P. 2066–2071. DOI: 10.1109/EIconRus49466.2020.9039255.

8. Kochedykov S.S., Dushkin A.V., Markin P.V. Express Assessment Method for the Risk of Impaired Functional Stability Information and Communication System in Conditions Cyber Attacks // 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2019. P. 1754–1757. DOI: 10.1109/EIConRus.2019.8657323.
9. Stouffer K., Pease M., Tang C., Zimmerman T., Pillitteri V., Lightman S., Hahn A., Saravia S., Sherule A., Thompson M. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Revision 3. 2023.
10. Воеводин В. А. Концептуальная модель объекта аудита информационной безопасности / В. А. Воеводин // Информация и безопасность. — 2019. — Т. 22, № 2. — С. 280–283.
11. Воеводин В. А. Эталонная модель объекта аудита информационной безопасности / В. А. Воеводин // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. — 2019. — № 9. — С. 56–61.

SOME APPROACHES TO THE DEVELOPMENT OF AN AUDIT RISK ASSESSMENT METHODOLOGY FOR THE INFORMATION SECURITY AUDIT OF CRITICAL INFORMATION INFRASTRUCTURE ENTITIES

Master's student Kochedykov S.S.

Moscow Institute of Electronic Technology

The article considers the task of developing an audit risk assessment methodology for auditing information security of subjects of critical information infrastructure. It is shown that the classical model of audit risk, based on inherent risk, the risk of controls and the risk of missing a significant discrepancy, requires clarification in relation to significant objects of critical information infrastructure. An approach is proposed in which the completeness of the implementation of mandatory security measures is considered not as an indicator independent of regulatory risk, but as a basis for its determination. To account for the heterogeneity of the elements of the critical information infrastructure object, a critically weighted risk of non-detection has been introduced, linking the final audit risk with the composition of the audit program. The methodology takes into account the category of significance, the state of implementation of mandatory security measures, the sustainability of critical functions, and the risk-oriented nature of the audit sample.

Keywords: information security audit, audit risk, audit certificate, significant object, critical information infrastructure, risk-based sampling, sustainability, FSTEC of Russia.



ОБЛАЧНЫЕ СЕРВИСЫ И БЕЗОПАСНОСТЬ ХРАНЕНИЯ ДАННЫХ

студ. Кузнецов Д.М.

Национальный исследовательский университет «МИЭТ»

В условиях стремительного развития цифровых технологий облачные сервисы становятся неотъемлемой частью информационно-технологической инфраструктуры предприятий, обеспечивая гибкость, масштабируемость и экономическую эффективность. Благодаря облачным технологиям теперь можно выполнять вычислительные услуги удаленно, даже если находиться в любой части города или мира. Все упомянутые полезные аспекты делают облачные вычисления предметом интереса многих научных кругов, а также отраслей промышленности. Поскольку в настоящее время значительная часть компаний переходит на облачные вычисления, безопасность данных становится более важной задачей.

Текущий механизм шифрование данных, возможно, не настолько надежен, чтобы обеспечить подлинную конфиденциальность и надежность. В данной статье предложено новое решение для защиты данных с использованием шифрования данных и метода хеширования паролей. Эффективность предложенного метода проверяется путем сравнения с текущим традиционным подходом к обеспечению безопасности на основе параметров безопасности.

1 Введение

Облачное хранилище – это одна из моделей хранения компьютерных данных. С его помощью данные хранятся на удаленных хранилищах, доступ к которым можно получить при помощи интернета. Про такие данные говорится, что они хранятся «в облаке». Физические удаленные хранилища охватывают несколько серверов, а управление физической средой обычно принадлежит хостинговой компании.

Развитие облачных хранилищ началось в начале 2000-х годов и с тех пор стремительно ускоряется. Сегодня всё больше компаний переходят на модели IaaS (Infrastructure as a Service), PaaS (Platform as a Service) и SaaS (Software as a Service), чтобы повысить гибкость и масштабируемость ИТ-инфраструктуры и снизить расходы.

В России также усиливается тренд на внедрение облачных технологий. Этому способствует внешнеполитическая обстановка: уход зарубежных поставщиков, сложности с импортом оборудования и ПО, а также требования регуляторов по использованию отечественных решений. В связи с этим вопросы информационной безопасности в облаке становятся ключевыми при выборе модели хранения данных и переноса инфраструктуры.

Рост рынка облачных услуг сопровождается увеличением числа атак на облачные ресурсы. В отличие от локальных систем, облачная среда требует специфических подходов к защите данных, управлению доступом, мониторингу угроз и выполнению нормативных требований. Риски – утечки данных, несанкционированный доступ, DDoS-атаки и ошибки в настройках – могут привести к серьезным финансовым и репутационным потерям.

Для того, чтобы это предотвратить, должны быть внедрены различные методы и техники для защиты данных, хранящихся в облаке. Сегодня все крупные и малые организации переходят на облачную модель работы с данными, где они могут столкнуться с рядом проблем, связанных, например, с хранением большого объема данных или их обработки. Качество данных в некоторых случаях может быть не на должном уровне. Однако их безопасность должна быть наиболее важной задачей среди всех других упомянутых проблем, связанных с данными. Поскольку это может привести к серьезным потерям или утечки конфиденциальных данных. Любой протокол защиты данных должен охватывать три основных принципа информационной безопасности, а именно конфиденциальность, целостность и доступность.

Конфиденциальность должна заключаться в том, что данные доступны только тем, кому они предназначены. Доступ к ним может получить только авторизованный пользователь, а не какой-либо злоумышленник. Данные должны быть точными в соответствии с принципом целостности. Данные должны быть доступны в любое время, когда это необходимо, это гарантируется принципом доступности. Поддержание всех этих параметров в сценарии внедрения облачных вычислений иногда является сложной задачей из-за их открытости и доступности. Все вышеперечисленное сильно мотивирует работать над аспектами защиты данных в облачной среде. Это может быть достигнуто за счет сочетания методов шифрования данных и хеширования.

2 Отличие подходов к обеспечению безопасности в облаке от традиционных подходов

В настоящее время активно используются облачные вычисления. Это привело к тому, что привычный подход к безопасности изменился. Облачная модель, как более современное решение, существенно отличается от классических методов защиты [1].

Если используется традиционная схема, хранение данных предусмотрено в локальной сети. В облачных же инфраструктурах, которые распределены и обслуживают сразу многих клиентов, требуется защищать большое количество модулей и приложений, гибко настраивать доступ, обеспечивать безопасность сетевого взаимодействия и предотвращать утечки между виртуальными средами.

Масштабирование. Облачные системы легко расширяются благодаря модульной архитектуре. Однако постоянные обновления и быстрые изменения, связанные с ростом компании, требуют непрерывного контроля уровня безопасности.

Взаимодействие с конечным пользователем. Облачные сервисы интегрируются с множеством других систем, поэтому нужно обеспечивать защиту на всех уровнях – от устройств пользователей до приложений и сетей. Важную роль играет своевременное управление правами доступа и отслеживание уязвимостей, возникающих из-за некорректных настроек и небезопасных установок.

Близость к другим данным и системам. Поскольку облако постоянно связано с клиентскими системами, уязвимость, которая возникла в одном компоненте, вполне может компрометировать всю среду. Провайдерам, которые хранят у себя данные, приходится использовать серьезные меры безопасности, так как они сами являются объектами риска.

3 Исследование методов защиты данных от утечки в облачных хранилищах

В результате анализа уязвимостей и угроз, с которыми сталкиваются облачные технологии в контексте обеспечения информационной безопасности, можно выделить несколько ключевых моментов. Представленная таблице 1 отражает систематизацию основных угроз, таких как утечка данных, атаки на облачную инфраструктуру, проблемы с аутентификацией и несанкционированный доступ. Каждый из этих факторов несет серьезные потенциальные последствия, такие как утрата конфиденциальности данных, финансовые потери, репутационные риски и недоступность сервисов. В таблице 1 отражено, что угрозы могут иметь как технические, так и организационные корни. Например, проблемы с аутентификацией и недостаточная защита API-интерфейсов могут привести к несанкционированному доступу и манипуляциям с данными. Нарушение контроля доступа и уязвимости в программном обеспечении создают угрозу для целостности и доступности сервисов. Так, приведенные угрозы и уязвимости подчеркивают важность комплексного подхода к обеспечению информационной безопасности в облачных сервисах. Это включает в себя как технические меры защиты (например, шифрование данных, внедрение многофакторной аутентификации), так и организационные (правильная настройка прав доступа, регулярное обновление программного обеспечения и патчей) [2]

Таблица 1

Уязвимости, риски и угрозы облачных технологий в контексте обеспечения ИБ облачных сервисов

№	Уязвимость/ Угроза	Описание	Последствия
1	Утечка данных	Ненадежное шифрование данных, утечка данных из-за ошибок настройки	Утрата конфиденциальности, финансовые потери, репутационные риски
2	Атаки на облачную инфраструктуру	DDoS-атаки, взлом сервисов, уязвимости в программном обеспечении	Прекращение работы облачных сервисов, потеря данных, недоступность сервисов
3	Проблемы аутентификации	Слабые пароли, отсутствие многофакторной аутентификации	Несанкционированный доступ, кража данных, вредоносное вмешательство
4	Несанкционированный доступ	Логин с украденными учетными данными, недостаточно жесткая защита прав доступа	Неавторизованные изменения в данных, разрушение целостности данных

5	Уязвимости API	Ненадежные API-интерфейсы без должной защиты	Проникновение через API, возможность манипуляций с данными
6	Нарушение контроля доступа	Ошибки в настройках прав доступа или их отсутствие	Неавторизованный доступ к системам и данным, нарушение работы сервисов
7	Уязвимости в программном обеспечении	Использование устаревших версий ПО, отсутствующие патчи	Эксплуатация уязвимостей, угроза целостности данных и работы сервисов

Чтобы обеспечить надежную безопасность облачных платформ, необходимо разработать комплекс стратегий для упреждающего устранения уязвимостей и рисков, связанных с облачными средами.

Шифрование играет ключевую роль в защите данных путем преобразования их в зашифрованный текст для предотвращения несанкционированного доступа. В облачных платформах есть две основные области, в которых применяется шифрование:

В состоянии покоя: это данные, которые не передаются активно с устройства на устройство или из сети в сеть, а хранящиеся на жестком диске, ноутбуке, флэш-накопителе или заархивированные/сохраненные каким-либо другим способом. Защита данных в состоянии покоя направлена на защиту неактивных данных, хранящихся на любом устройстве или в сети. Хотя такие данные иногда считаются менее уязвимыми, чем данные в процессе передачи, злоумышленники часто считают их более ценной целью, чем данные в движении. Профиль риска зависит от мер безопасности, которые применяются для защиты данных в любом состоянии.

При передаче: Данные, перемещающиеся между клиентскими устройствами и облачными серверами или между различными частями облачной инфраструктуры, подвержены перехвату. Шифрование этих данных при передаче с использованием таких протоколов, как TLS, гарантирует, что они остаются конфиденциальными [3].

При использовании: В сценариях, где данные активно обрабатываются или используются, исследуются методы шифрования, такие как гомоморфное шифрование, для поддержания конфиденциальности данных, позволяя выполнять вычисления без необходимости расшифровки, тем самым снижая потенциальные риски.

Стратегия смягчения последствий: стоит принять стандарты шифрования, такие как AES-256, и передовые методы управления ключами для защиты ключей шифрования от их утечки. [4].

Шифрование данных обеспечивает конфиденциальность и целостность информации как при ее хранении, так и при передаче, что значительно снижает риски утечек и перехвата данных.

4 Предложенная методология

В этом разделе будет подробно рассмотрено предлагаемое новое решение для защиты облачных данных. В нем будут рассмотрены как современные подходы к обеспечению безопасности, так и предлагаемое решение.

А. Предлагаемый подход к обеспечению безопасности данных

В этом разделе два разных метода были объединены для обеспечения максимальной безопасности данных в облаке. Этими методами являются шифрование данных и хэширование закрытого ключа с помощью соли.

Шифрование данных – это преобразование данных в зашифрованную форму с помощью открытого ключа шифрования, и которые находятся в нечитаемом виде до тех пор, пока не будут возвращены к исходному виду с помощью закрытого ключа. Процесс шифрования данных перед загрузкой в облачное хранилище позволяет легко сохранить конфиденциальность данных. В данной статье будет использоваться метод асимметричного шифрования, при котором ключ шифрования является открытым, поэтому он может быть доступен многим людям, которые работают в одной организации, чтобы они могли зашифровать данные перед их загрузкой в облако. Закрытый ключ при асимметричном методе шифрования хранится в секрете, поэтому он доступен только выбранному пользователю, с которым организация хочет поделиться данными.

Зашифрованные данные, хранящиеся в облаке, защищены с помощью специальных ключей. Но сегодня пароли можно взломать, используя различные подходы, такие как атака методом перебора, атака по словарю, таблицы поиска, таблицы обратного поиска, радужные таблицы и т.д. Все это простые, но эффективные методы, которые злоумышленники используют для взлома.

Для решения проблемы безопасности паролей в облаке предложено использовать хэш-функцию, которая является односторонней функцией, с использованием соли. Хэш-функция – это математическая функция, которая принимает на вход произвольные данные любой длины, а на выходе получает строку со строго определенным числом символов. Хэш-функция имеет лавинный эффект, в рамках которого существенная корректировка выходного значения становится возможной даже при небольшом изменении входной информации [5]. Более подробное описание этого подхода приведено в следующем разделе.

В. Внедрение нового алгоритма защиты данных

Данные в облаке шифруются с использованием асимметричного шифрования, при котором ключ шифрования является открытым, а ключ расшифрования – закрытым.

- 1) Генерация закрытого ключа
- 2) Генерация длинной случайной соли, используя криптографический стойкий генератор псевдослучайных чисел;
- 3) Присоединение соли к закрытому ключу и хэширование с помощью стандартной криптографической хэш-функции, например, SHA256, SHA512, Ripe MD или ГОСТ 34.11-2018;

Сохраняем и соль, и хэш-код в записи базы данных пользователей (рисунок 1).

Это самый надежный способ сохранить данные в облаке. Если хакер попытается взломать закрытый ключ цифровой подписи из зашифрованных данных наиболее эффективным способом может быть взломан только закрытый ключ. Но поскольку аутентификация основана на полученном хэш-коде, данные не могут быть расшифрованы ни при каких условиях. Секретная информация будет предоставлена поставщиком облачных услуг, а закрытый ключ будет храниться в безопасности у уполномоченного лица.

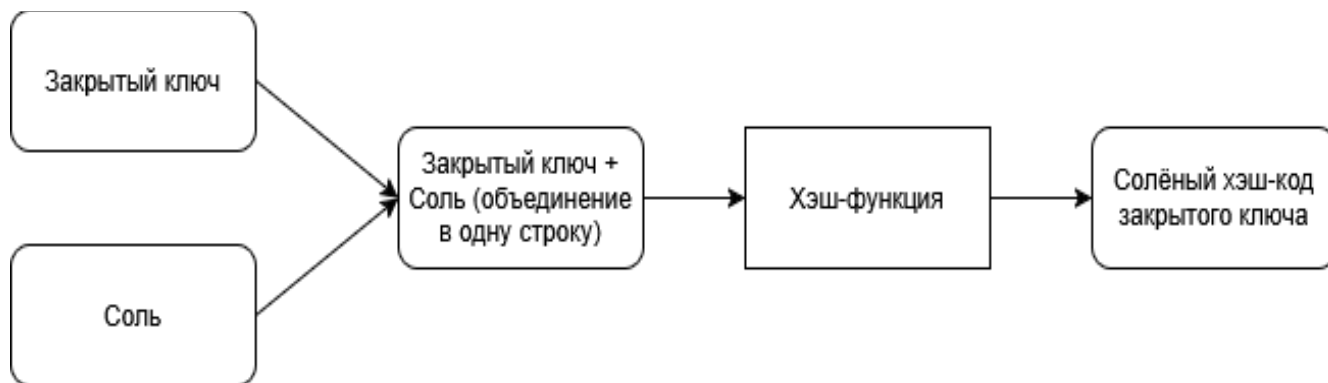


Рисунок 1 – Солёный хэш-код закрытого ключа

3) Аутентификация по ключу и доступ к данным:

Заключительным этапом является получение доступа к данным из облака. Пользователь отправляет запрос на облачный сервер для получения данных, вводя свой приватный ключ. Если запрашиваемый файл существует и приватный ключ введён верно, облачный сервер выбирает соответствующую «соль» и вычисляет её хэш-код. Затем этот хэш-код повторно обрабатывается вместе с хэшем введённого приватного ключа. Если полученный итоговый ключ совпадает с ключом расшифрования, пользователь проходит аутентификацию, после чего данные расшифровываются и предоставляются пользователю.

Таким образом, резюмируя всю процедуру, данные отправителя сначала шифруются с использованием шифрования с открытым ключом. Затем зашифрованные данные будут загружены на облачный сервер, который обеспечит безопасность и конфиденциальность данных. Загруженные зашифрованные данные могут быть загружены из облака и расшифрованы обратно с помощью хэшированного закрытого ключа. Здесь данные могут быть расшифрованы обратно пользователем, прошедшим проверку подлинности, у которого есть закрытый ключ. Обобщенная идея хранения данных в облаке и доступа к ним оттуда более наглядно проиллюстрирована на рисунке 2

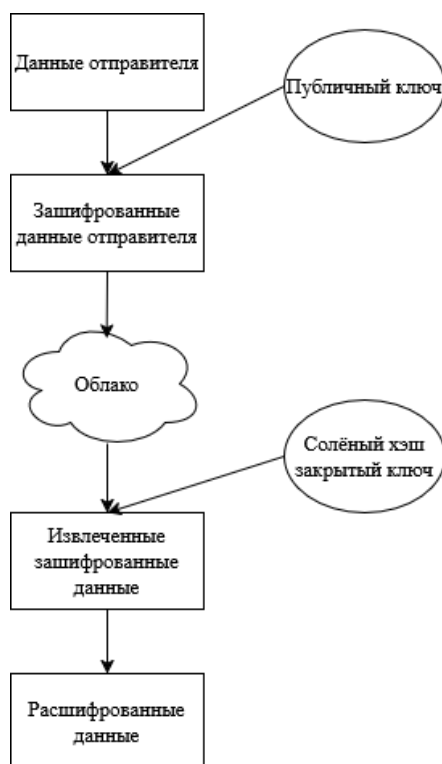


Рисунок 2 – Хранение данных и доступ к ним

После реализации предложенной идеи безопасность облачных данных будет улучшена. В следующей таблице 2 показано сравнение производительности системы, реализованной без защиты, традиционных методов защиты, которые используются в настоящее время, и предложенного метода. Здесь сравнение приведено в таблице на основе нескольких важных параметров безопасности, а именно аутентификации, конфиденциальности, доступности, конфиденциального характера, защищенности и надежности [6].

Таблица 2

Сравнение параметров безопасности

Параметры безопасности	Результат		
	Без защиты	Традиционный метод защиты	Предложенный метод
Аутентификация	Нет	Единичная	Двойная
Доступность	Низкая	Высокая	Высокая
Конфиденциальность	Низкая	Средняя	Высокая
Защищенность	Низкая	Средняя	Высокая
Надежность	Низкая	Высокая	Высокая

5 Заключение

Защита данных в инфраструктуре облачных вычислений является одной из наиболее важных проблем, которую можно решить более эффективно, используя криптографические методы. Здесь, в этой статье, было предложено новое решение, объединив два различных метода, один из которых – асимметричное шифрование данных, а другой – солёное хэширование паролей, для устранения угроз безопасности. Согласно данному подходу, сначала данные пользователя шифруются с помощью открытого ключа, а затем закрытый ключ хэшируется с помощью случайной соли, чтобы сделать закрытый ключ безопасным, а шифрование – нерушимым. Предлагаемый метод быстр и надежен. Шифрование может значительно снизить риск кражи данных в глобальном масштабе и утечки данных из облака. В последнее время мы переходим к облачной инфраструктуре для хранения наших личных данных. Таким образом, обеспечение безопасной среды действительно необходимо для адаптации новой облачной технологии.

Литература:

1. Зонова Дарья Юрьевна Способы защиты облачных хранилищ // Colloquium-journal. 2024. №2 (195). URL: <https://cyberleninka.ru/article/n/sposoby-zaschity-oblachnyh-hranilisch> (дата обращения: 01.04.2026).
2. Тимонин Вадим Андреевич, Уткин Александр Владимирович, Козлова Юлия Дмитриевна Уязвимости и риски облачных технологий в контексте обеспечения информационной безопасности облачных сервисов // Парадигма. 2025. №3-2. URL: <https://cyberleninka.ru/article/n/uyazvimosti-i-riski-oblachnyh-tehnologiy-v-kontekste-obespecheniya-informatsionnoy-bezopasnosti-oblachnyh-servisov> (дата обращения: 01.04.2026).
3. Самадхан Кадам. Шифрование данных: концепция и инструменты. // Medium.com, 2019. [Электронный ресурс] Режим доступа: <https://medium.com/petabytz/data-encryption-concept-tools-cebf03a87b34>
4. Снитовец А. В. Стратегии минимизации угроз и инцидентов в облачных платформах // Актуальные исследования. 2023. №36 (166). С. 28-38. URL: <https://apni.ru/article/6967-strategii-minimizatsii-ugroz-i-intsidentov>
5. [«Криптография в блокчейнах»: о хеш-функциях, ключах и цифровых подписях. – 2020. [Электронный ресурс]. – URL: <https://habr.com/ru/companies/bitfury/articles/327272/> (дата обращения 2026-31-03).
6. Ghosh, Soumalya, Anubhav Raj Singh, Garima Pandey, Anupam Lakhanpal. A Novel Solution to Cloud Data Security Issues. // 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2020.

CLOUD SERVICES AND SECURE DATA STORAGE ISSUES

student. Kuznetsov D.M.

National Research University "Moscow Institute of Electronic Technology"

With the rapid development of digital technologies, cloud services are becoming an integral part of the information technology infrastructure of enterprises, providing flexibility, scalability and cost-effectiveness. Thanks to cloud technologies, it is now possible to perform computing services remotely, even if you are located in any part of the city or the world. All these useful aspects make cloud computing a subject of interest for many scientific circles, as well as industries. As a significant number of companies are currently switching to cloud computing, data security is becoming more important.

The current data encryption mechanism may not be reliable enough to ensure genuine confidentiality and reliability. This article offers a new solution for data protection using data encryption and password hashing. The effectiveness of the proposed method is checked by comparing it with the current traditional approach to ensuring security based on security parameters.



ОБНАРУЖЕНИЕ АНОМАЛИЙ В КОНТЕЙНЕРИЗИРОВАННЫХ СРЕДАХ

асп. Кеньков Е. А., доц. Лапина М. А.

Северо-Кавказский федеральный университет,

Контейнеры стали стандартом для современных информационных систем, однако все еще имеют проблемы с безопасностью. Мониторинг системных вызовов помогает замечать атаки, но традиционные детекторы часто срабатывают на единичные события и дают много ложных тревог. В данной работе предпринята попытка оценить, насколько эффективно популярные простые классификаторы справляются с задачей при анализе каждого системного вызова изолированно. Предлагаемый подход основан на сравнении четырех алгоритмов классификации: логистическая регрессия, метод опорных векторов, случайный лес и градиентный бустинг – на размеченном наборе данных, содержащем системные вызовы, энергопотребление, загрузку процессора и использование памяти. Дополнительно проводится анализ переходов между соседними вызовами для выявления возможных аномальных цепочек системных вызовов. Для этого строятся пары «текущий вызов – следующий вызов», вычисляются отношения частот встречаемости в аномалиях к частотам в норме, после чего строится тепловая карта логарифмов этих отношений. Результатом является доказательство того, что использование записи о каждом системном вызове по отдельности ведёт к переобучению модели под энергопотребление, что снижает надёжность классификации в реальных условиях.

Введение

Контейнеризация, как частная форма виртуализации, является технологией, которая достаточно подвержена атакам и имеет множество уязвимостей [1][2]. Но кроме того, что данные уязвимости нужно вовремя устранять, также необходимо уметь вовремя обнаруживать возможные аномалии в работе контейнеров, которые могут приводить к нарушению целостности, конфиденциальности и доступности данных, хранящихся и обрабатываемых в контейнерах.

Одним из популярных способов выявления аномалий является анализ системных вызовов контейнера [3]. Так как контейнеры общаются с ядром хостовой операционной системы через системные вызовы (syscall), которые складываются в цепочку, то их конечно же можно перехватывать и анализировать. Анализ может происходить как по одиночке, так и части непрерывной цепочки [4].

В исследовании [5] авторы предложили использовать для обнаружения аномалий не последовательности вызовов, а Bag of System Calls (BoSC). Идея использования BoSC заключается в том, что отбрасывается порядок следования вызовов, остаются только частоты каждого типа syscall в рамках одного процесса. В данной работе для обучения также использовались метод опорных векторов и логистическая регрессия и получили лучшие результаты.

В статье [6] авторы представляют детектор аномалий на системных вызовах, но вместо BoSC они преобразуют последовательность вызовов во взвешенный ориентированный граф. Из графа извлекают компактное описание поведения контейнера, а затем подают его на ансамбль из двух моделей – случайного леса (Random Forest) и изолирующего леса (Isolation Forest). Такое сочетание должно распознавать более тонкие аномалии, чем обычная классификация. Эксперименты проводили в контролируемой среде на двух самых распространённых типах угроз для облачных контейнеров. Результаты показали отличный результат и низкий уровень ложных срабатываний.

В данной работе не используются методы скользящего окна и BoSC, так как задача исследования заключается в том, чтобы понять, насколько может быть информативной отдельная запись о системном вызове, насколько эффективны алгоритмы машинного обучения для классификации таких одиночных записей и можно ли визуально при помощи тепловой карты находить аномалии в двух идущих друг за другом системных вызовах.

Для этого были обучены четыре популярных классификатора: логистическая регрессия (Logistic Regression), метод опорных векторов (SVM), случайный лес (Random Forest) и градиентный бустинг (Gradient Boosting) – которые обрабатывают информацию о каждом системном вызове независимо.

Также была составлена тепловая карта системных вызовов, которая показывает, как пара системных вызовов, следующих друг за другом могут указывать на возможные аномалии, а также позволяет понять, какие пары syscall чаще встречаются именно в аномалиях.

Данные и постановка задачи

Для проведения классификации и построения тепловой карты был выбран набор данных «OS Kernel Anomaly Dataset» с сайта kaggle размером в тысячу записей, и каждая запись содержит информацию об одном системном вызове.

В одной записи содержится временная метка (Timestamp), имя системного вызова (Syscall), идентификатор процесса (PID), название процесса (Process_Name), энергопотребление в ваттах (Power_W),

загрузка CPU в процентах (CPU_Usage_%), используемая память в мегабайтах (Mem_Usage_MB) и классификационная метка (Label), которая имеет значение Normal или Anomaly. Всего в выборке ровно 91% нормальных событий и 9% аномалий. Системных вызовов встречается семь типов: read, open, close, write, ioctl, execve, mmap.

Перед тем как обучать модели, была сделана простая предобработка. Для начала была перекодирована классификационная метка в бинарный формат, где Normal был сопоставлен с 0, а Anomaly с 1. Далее категориальный признак Syscall был преобразован в набор фиктивных переменных, создав тем самым 7 дополнительных столбцов, так как алгоритмы машинного обучения плохо понимают текст [7]. К ним добавили числовые признаки Power, CPU и Mem. В итоге на каждый объект приходится десять признаков. Остальные признаки были отброшены, так как не несли практической ценности для обучения моделей в рамках данного исследования.

После обработки набора данных задача свелась к классической бинарной классификации, так как отсутствует временная зависимость между разными PID и не используется идентификатор процесса, потому что цель проверить, можно ли выявить аномалию по единичным записям системных вызовов.

Для создания тепловой карты последовательностей был выбран иной подход. В первую очередь были отсортированы события по времени внутри каждого PID и для каждого вызова был записан следующий за ним вызов. Таким образом получились пары (syscall, next_syscall). Если у процесса был только один вызов или он последний – такую пару не учитывали. Потом все пары были сгруппированы на нормальные и аномальные в зависимости от метки первого вызова в паре. После чего для каждого из семи типов syscall была построена матрица переходов, которая, например, содержала в себе информацию о том, сколько раз после open встретился read, или после execve был вызван mmap. Далее для сравнения нормальных и аномальных матриц были взяты отношения их вероятностей, и если их отношение выше единицы, то данная пара системных вызовов представляет собой аномальное поведение. Также для большей наглядности на графике был взят логарифм по основанию 2 для каждого отношения, чтобы значения отношений не сильно превышали единицу.

Проведение исследования

Для исследования были взяты четыре популярные модели для классификации. Logistic Regression была выбрана как самый простой линейный метод классификации. SVM же способен улавливать нелинейности, что может положительно повлиять на результат. Random Forest и Gradient Boosting являются ансамблями деревьев, и они достаточно хорошо работают с табличными данными. Параметры для данных моделей использовались по умолчанию, кроме указания class_weight='balanced' для логистической регрессии, SVM и случайного леса, чтобы модель не игнорировала редкий класс аномалий.

Выборка случайным образом была разбита на две части, где 80% использовались для обучения, а оставшиеся 20% – для проверки. При этом доли аномалий в обеих частях сохранили одинаковыми, чтобы тест не оказался слишком простым.

Результат оценки предсказаний на тестовой выборке представлен в таблице 1. Из нее можно сделать вывод, что accuracy у всех моделей выше 87%, а у Gradient Boosting даже 93%. Но полнота (recall) у Gradient Boosting и Random Forest очень низкая. Это может говорить о том, что ансамбли деревьев пропускает практически половину реальных аномалий. В свою очередь Logistic Regression и SVM имеют одинаково высокую полноту со значением 0.833, но, к сожалению, показывают низкую точность (precision). Это значит, что они часто ошибаются и называют нормальные события аномальными. Для реального детектора это неприемлемо, потому что ложных тревог будет больше, чем истинных.

Таблица 1

Результаты оценки предсказаний моделей классификации

Модели	Accuracy	Recall	Precision	F1
Logistic Regression	0.88	0.833	0.417	0.556
SVM	0.875	0.833	0.405	0.545
Random Forest	0.925	0.5	0.6	0.545
Gradient Boosting	0.93	0.667	0.6	0.632

По итогу самую высокую оценку F1 получил Gradient Boosting, равную 0.632. И матрица ошибок для Gradient Boosting представлена в таблице 2.

Таблица 2

Матрица ошибок для Gradient Boosting

	Actually Positive	Actually Negative
Predicted Positive	12	6
Predicted Negative	8	174

Из 200 тестовых данная модель классификации верно определила 174 нормальных и 12 аномальных записей, но 8 нормальных записей она приняла за аномалии, а 6 аномалий пропустила.

Из этого можно сделать вывод, что низкая точность у линейных моделей и невысокая полнота у леса говорят о том, что признаки не идеальны, но добавление времени в контекст может улучшить результаты.

Но важным замечанием к Gradient Boosting является то, что самым важным признаком для него является энергопотребление (Power_W), и его важность составляет 0,617. А в то же время суммарная важность бинарных признаков системного вызова (Syscall) составляет 0,014. Это означает, что модель в большинстве своем ориентировалась на энергопотребление, что доказывает, почему у нее такой высокий показатель ассигасы, ведь аномалии обычно сопровождаются скачками энергопотребления.

По своей сути настоящая атака на контейнер является цепочкой действий, но ранее рассматриваемые классификаторы обучались и делали предсказания для каждого syscall изолированно. Поэтому было решено проверить, можно ли выявить аномалии по переходам между системными вызовами.

Тепловая карта (рисунок 1) показывает эти соотношения. Более темные оттенки показывают переходы, которые являются индикаторами аномалий. Самые яркие пятна получились у пар open-execve, так как злоумышленник может открыть файл и сразу запустить его содержимое, write-execve из-за того, что злоумышленник может записать вредоносный скрипт в файл и сразу его запустить, и ioctl-mmap, так как может являться признаком того, что производится подготовка к атаке через DMA (Direct Memory Access) или обходом защит потому, что ioctl часто используется для управления устройствами, а mmap используется для отображения памяти. Такие паттерны являются типичным для эксплуатации уязвимости. У нормальных процессов таких переходов почти нет, так как они чаще работают по одному и тому же сценарию: read-read, write-write, write-read и редко open-close.

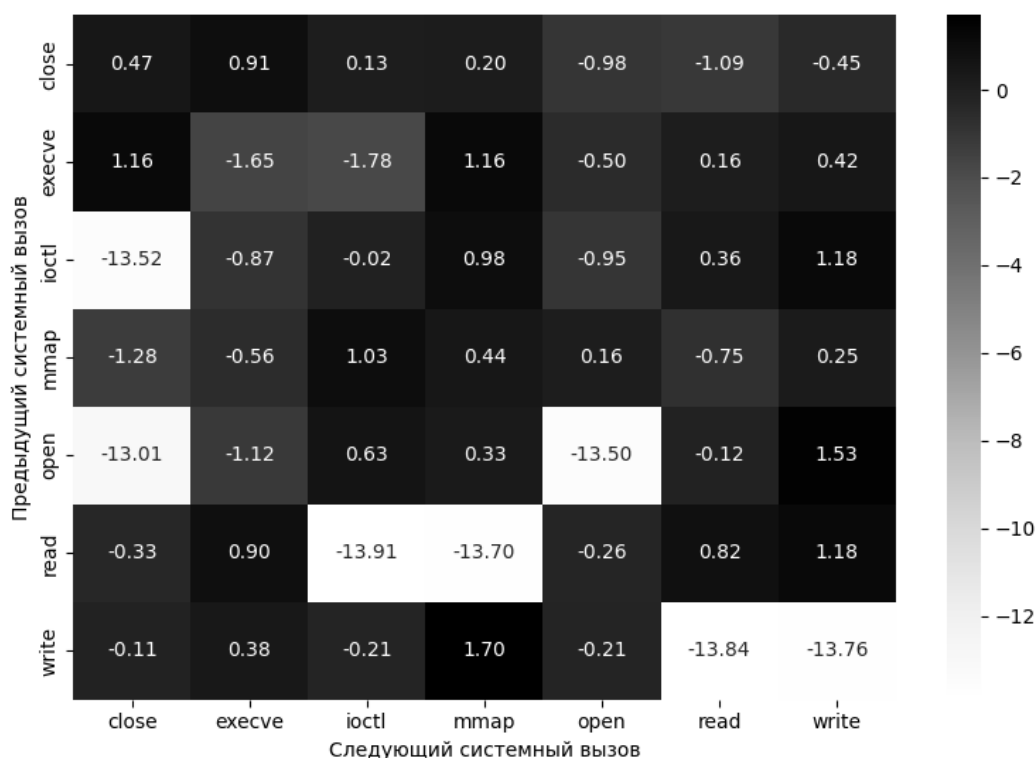


Рисунок 1 – Тепловая карта системных вызовов.

Важно также заметить, что выводы по тепловой карте в целом достаточно близки с интуитивными, ведь атака в контейнере обычно следует сценарию загрузки вредоносного файла (open), далее идет его запуск (execve), после записывается результат атаки (write) и завершается работа с файлами или вводом-выводом (close). И как раз-таки в полученной в данном исследовании тепловой карте пара open-execve выделяется, а execve-write тоже немного выше нормы. Поэтому из полученного результата следует, что для получения

полной картины атаки не хватает длины цепочки, так как два подряд идущих системных вызова хоть и не так мало информативны, как один, но контекста все еще не хватает.

Анализ последовательностей показал, что аномалии не случайны. Они образуют устойчивые пары и тройки вызовов, которые можно выучить. При этом примечательно, что ни один из классификаторов из первой части не увидел данных переходов, так как они работали с отдельными событиями. И даже обычный анализ пар `syscall` выявляет характерные для аномалий паттерны, хоть он и не даёт численных метрик вроде F1.

Выводы

Был взят размеченный датасет логов системных вызовов с метриками ресурсов и опробованы два подхода к обнаружению аномалий. Первый подход представлял собой такие классификаторы, как Logistic Regression, SVM, Random Forest, Gradient Boosting. Второй являлся визуальным анализом переходов между последовательными `syscall`.

По итогу Gradient Boosting дал лучшую оценку F1 (0,632), и это ненадёжная опора для реальной системы. При этом ассигасу оказалась высокой (0,93), что обманчиво, так как за ней скрывается низкая полнота на аномалиях. Можно сказать, что модель чаще перестраховывается и предсказывает отсутствие аномалии, если сомневается. Именно поэтому оценка `recall` составила всего 0,667, а это значит, что почти треть аномалий осталась незамеченной.

Также модель практически не обращала внимания на тип системного вызова, так как параметр `Power_W` оказался в 20 раз важнее, чем любой бинарный флаг `syscall`. В реальном контейнерном окружении энергопотребление зависит от таких факторов как соседние контейнеры, утилизация CPU, состояние кэшей. И если ответ модели опирается в основном на потребление энергии, то он будет давать сбои при малейшем изменении нагрузки.

А анализ переходов же выявил чёткие аномальные паттерны: `open-execve`, `write-execve`, `ioctl-mmap` – которые не зависят от энергопотребления. Это означает, что если бы в контекст модели был добавлен не только текущий `syscall`, но и предыдущий, полнота могла бы вырасти без привязке к ваттам. Простым и логичным решением этой проблемы является использование скользящего окна из двух или трёх системных вызовов. Это решение не сильно бы увеличило сложность, но зато предоставила бы модели временной контекст.

И из данного исследования можно сделать вывод, что для небольших размеченных наборов данных простой анализ переходов между `syscall` даёт понятные и интерпретируемые сигнатуры атак. А классификатор без контекста, который включает в себя время, часто даёт неправильную оценку и может ориентироваться больше на энергопотребление, чем на системные вызовы.

Благодарности.

**Исследование выполнено за счет гранта Российского научного фонда № 25-71-30007,
<https://rscf.ru/project/25-71-30007/>.**

Литература

1. Lee H., Kwon S., Lee J. H. Experimental analysis of security attacks for Docker Container Communications //Electronics. – 2023. – Т. 12. – №. 4. – С. 940.
2. Wong A. Y. et al. Threat modeling and security analysis of containers: A survey //arXiv preprint arXiv:2111.11475. – 2021.
3. El Khairi A. et al. Contextualizing system calls in containers for anomaly-based intrusion detection //Proceedings of the 2022 on Cloud Computing Security Workshop. – 2022. – С. 9-21.
4. Cavalcanti M., Inacio P., Freire M. Performance evaluation of container-level anomaly-based intrusion detection systems for multi-tenant applications using machine learning algorithms //Proceedings of the 16th International Conference on Availability, Reliability and Security. – 2021. – С. 1-9.
5. Kang D. K., Fuller D., Honavar V. Learning classifiers for misuse and anomaly detection using a bag of system calls representation //Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop. – IEEE, 2005. – С. 118-125.

6. Iacovazzi A., Raza S. Ensemble of random and isolation forests for graph-based intrusion detection in containers //2022 IEEE International Conference on Cyber Security and Resilience (CSR). – IEEE, 2022. – С. 30-37.
7. Carrizosa E., Restrepo M. G., Morales D. R. On clustering categories of categorical predictors in generalized linear models //Expert Systems with Applications. – 2021. – Т. 182. – С. 115245.

ANOMALY DETECTION IN CONTAINERIZED ENVIRONMENTS

PhD student Kenkov E. A., PhD, assoc. prof. Lapina M. A.

North-Caucasus Federal University, Stavropol

Containers have become the standard for modern information systems, but they still pose security challenges. System call monitoring helps detect attacks, but traditional detectors often trigger on isolated events and generate numerous false alarms. This paper attempts to evaluate the effectiveness of popular simple classifiers when analyzing each system call in isolation. The proposed approach is based on a comparison of four classification algorithms—logistic regression, support vector machines, random forests, and gradient boosting—on a labeled dataset containing system calls, power consumption, CPU load, and memory usage. Additionally, transitions between adjacent system calls are analyzed to identify potential anomalous chains of system calls. This is accomplished by constructing "current call – next call" pairs, calculating the ratios of anomaly frequencies to normal frequencies, and then constructing a heat map of the logarithms of these ratios. The result is evidence that using a record of each system call individually leads to overfitting the model for power consumption, which reduces the reliability of classification in real-world conditions.



ИМИТАЦИОННАЯ МОДЕЛЬ КАНАЛА ПЕРЕХВАТА ПЭМИ ИНТЕРФЕЙСА VGA ДЛЯ ИССЛЕДОВАНИЯ ВЛИЯНИЯ ПОЛОСЫ ПРОПУСКАНИЯ ПРИЕМНОГО УСТРОЙСТВА НА РАСПОЗНАВАНИЕ ТЕКСТА

преп. Лукманова О.Р.

Национальный исследовательский университет «МИЭТ»

В статье представлена разработанная в среде MATLAB имитационная модель канала перехвата побочных электромагнитных излучений видеосистем с интерфейсом VGA. Модель включает модули синтеза тестового изображения, генерации VGA-сигнала, формирования и распространения ПЭМИ, приемного устройства и восстановления изображения. Исследовано влияние полосы пропускания приемного устройства RBW на качество восстановления текстовых изображений. Показано, что уменьшение RBW приводит к сглаживанию фронтов видеосигнала, снижению контраста и ухудшению разборчивости символов. Установлено, что максимальные значения SNR достигаются при $RBW \approx 0,7f_n$, а при $SNR \geq 15$ дБ вероятность распознавания текста становится близкой к 100%. Результаты могут использоваться при оценке угроз утечки информации по каналу ПЭМИ.

Побочные электромагнитные излучения (ПЭМИ) средств вычислительной техники (СВТ) создают потенциальный канал утечки информации, позволяющий восстанавливать изображение с экрана монитора [1, 2]. Наиболее информативными являются аналоговые видеосистемы с интерфейсом VGA (Video Graphics Array), широко распространенные в составе промышленного и офисного оборудования [3].

Практический интерес представляет восстановление текстовой информации, качество которого определяется уровнем ПЭМИ, расстоянием перехвата и полосой пропускания приемного устройства RBW [1–3]. Уменьшение RBW приводит к ослаблению высокочастотных составляющих видеосигнала, снижению контраста и разборчивости текста, тогда как чрезмерное расширение полосы повышает уровень шума. Поэтому актуальна разработка имитационной модели, позволяющей исследовать влияние RBW на качество восстановления текстовых изображений. Разработанная в среде MATLAB модель реализует программное представление канала перехвата ПЭМИ видеосистемы VGA и построена по модульному принципу (рисунок 1).

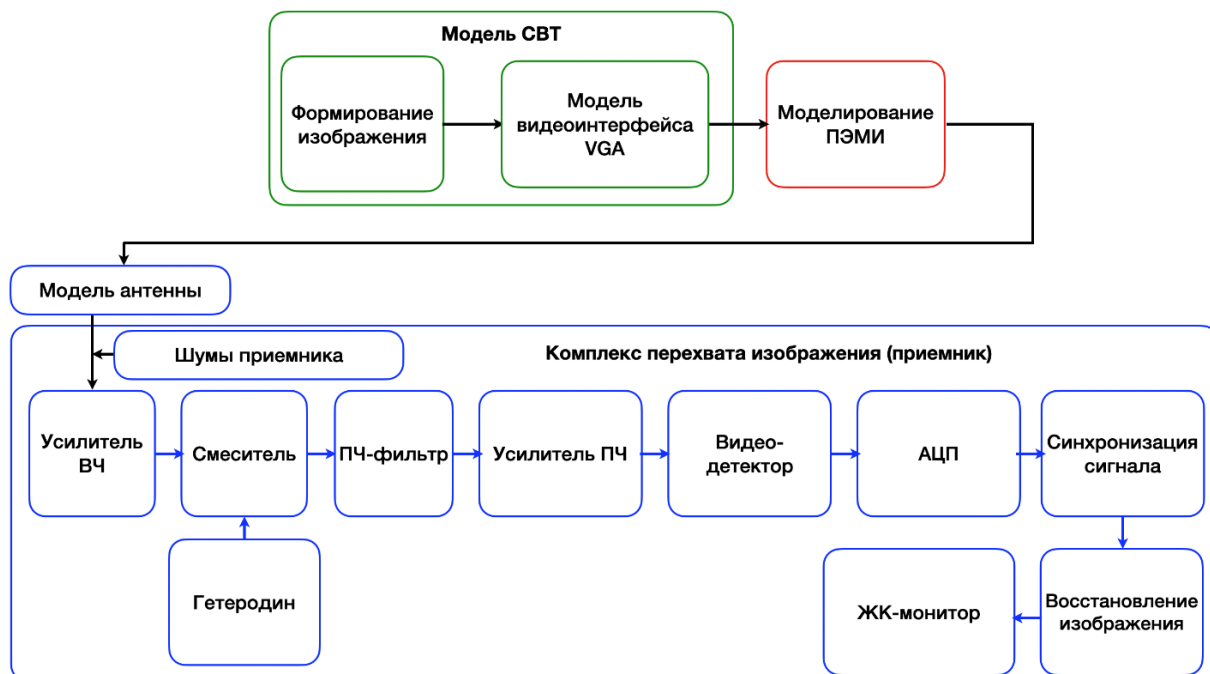


Рисунок 1 – Структурная схема виртуального лабораторного стенда для моделирования канала перехвата ПЭМИ видеосистем VGA

Эталонное изображение формируется в формате Full HD (1920×1080 пикселей) и в цифровой области представляется трехмерным массивом данных, соответствующим аддитивной цветовой модели RGB:

$$I = \{I(x, y, c)\}, \quad x = 1 \dots 1920, \quad y = 1 \dots 1080, \quad c \in \{R, G, B\}, \quad I(x, y, c) \in [0; 1]. \quad (1)$$

Нулевое значение элемента массива соответствует черному уровню, единичное – белому уровню. В качестве тестового изображения используется набор строчных букв русского алфавита, набранных шрифтом Times New Roman кеглем 14 пунктов. Для оценки влияния масштаба текст выводится в вариантах 75 %, 125 % и 250 % (рисунок 2).

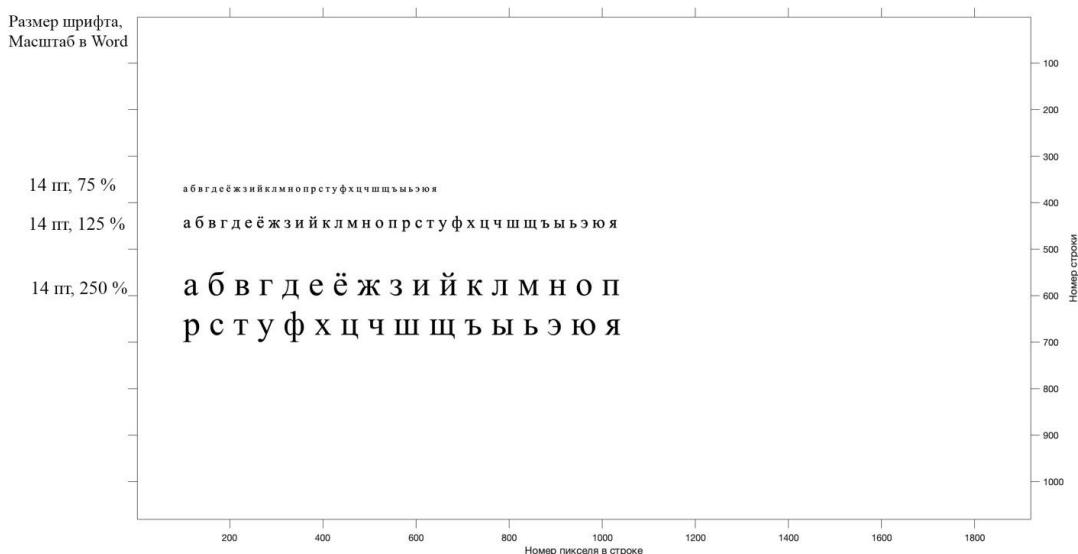


Рисунок 2 – Синтезированное эталонное Full HD-изображение с кириллическим текстом

Генерация видеосигнала выполняется в соответствии с параметрами стандарта VESA Coordinated Video Timings для разрешения 1920×1080 при частоте обновления 60 Гц [4]. Пиксельная тактовая частота составляет $f_{\text{п}} = 172,75$ МГц, что соответствует длительности элементарного интервала $T_{\text{п}} = 1/f_{\text{п}} \approx 5,79$ нс. По горизонтали строка содержит 1920 пикселей активной области, 120 пикселей переднего гасящего интервала, 208 пикселей синхроимпульса и 328 пикселей заднего гасящего интервала, что в сумме составляет 2576 пикселей, или 14,912 мкс. По вертикали кадр включает 1080 активных строк, 1 строку переднего гасящего интервала, 3 строки синхроимпульса и 34 строки заднего гасящего интервала; общая структура кадра составляет 1118 строк, или 16,671 мс. Пример осциллограммы фрагмента VGA-сигнала приведен на рисунке 3.

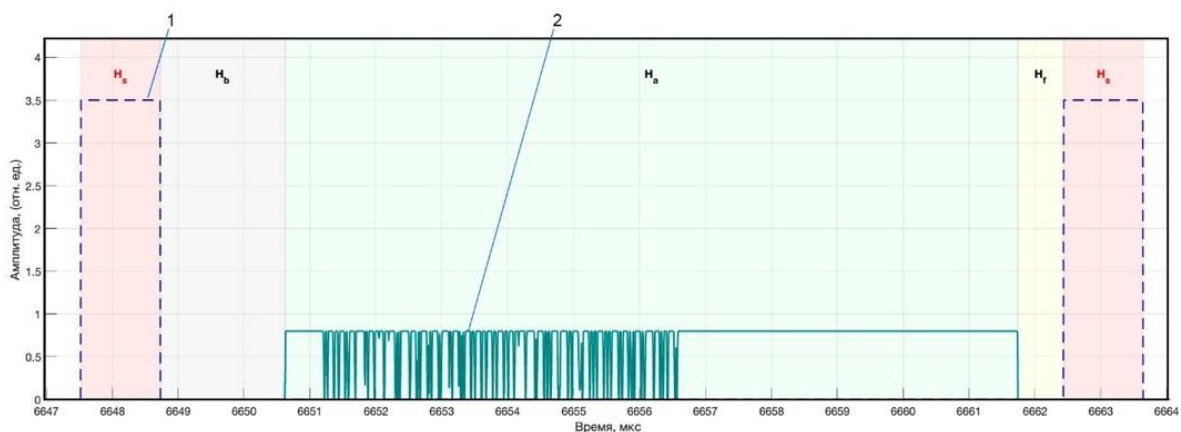


Рисунок 3 – Детализированная осциллограмма одной строки VGA-сигнала: канал строчных синхроимпульсов H_s (1); канал видеоданных Green (2)

Комплексный VGA-сигнал формируется как суперпозиция цветных каналов R, G, B и синхроимпульсов. В модели приняты уровни: активная область видеоданных – 0,8 В, синхроимпульсы – 3,5 В. Последовательная передача значений пикселей определяет спектральный состав ПЭМИ и, следовательно, требования к полосе пропускания приемного устройства.

Видеокабель моделируется как случайная антенна с калибровочным коэффициентом $K_{a.сл}(f)$, измеренным экспериментально в безэховой камере на расстоянии 1 м [3].

Напряженность электрического поля $E(f)$ на расстоянии 1 м:

$$E(f) = U(f) + K_{a.сл}(f), \quad (2)$$

где $U(f)$ – напряжение информативного сигнала на частоте f , дБ(мкВ).

Затухание в свободном пространстве на расстоянии r рассчитывается по формуле [5]:

$$V(f, r) = 20 \log_{10} \left(\frac{r_0}{r} \right)^3 \cdot \sqrt{\frac{k_f^4 r^4 - k_f^2 r^2 + 1}{k_f^4 r_0^4 - k_f^2 r_0^2 + 1}}, \quad (3)$$

где $V(f, r)$ – коэффициент ослабления ПЭМИ на расстоянии r на частоте f ; $k_f = 2\pi f/c$ – волновое число; $c = 3 \cdot 10^8$ м/с – скорость света; r_0 – расстояние, на котором производилось измерение ПЭМИ ($r_0 = 1$ м).

С учетом формулы (3) напряженность электромагнитного поля ПЭМИ на расстоянии r от СТВ можно рассчитать по формуле:

$$E_r(f) = E(f) + V(f, r). \quad (4)$$

Модель приемного устройства построена с учетом характеристик анализатора спектра R&S®FSW и активной всенаправленной антенны R&S®HE600 [6, 7]. В расчете учитываются спектральная плотность собственных шумов анализатора, калибровочный коэффициент приемной антенны и ее спектральная чувствительность.

Спектр сигнала на входе приемного устройства представляет собой суперпозицию информативной составляющей, шумов приемной антенны и собственных шумов анализатора.

Принятый сигнал усиливается радиочастотным каскадом и поступает на смеситель, где выполняется преобразование частоты с использованием гетеродина. Частота гетеродина определяется выбранной центральной частотой настройки $f_0 = 172,75$ МГц и промежуточной частотой $f_{пч} = 250$ МГц. Для выделения информативной составляющей применен полосовой фильтр Баттерворта второго порядка с перестраиваемой полосой RBW. Спектр и осциллограмма сигнала на выходе полосового фильтра (RBW = 172,75 МГц) приведены на рисунке 4.

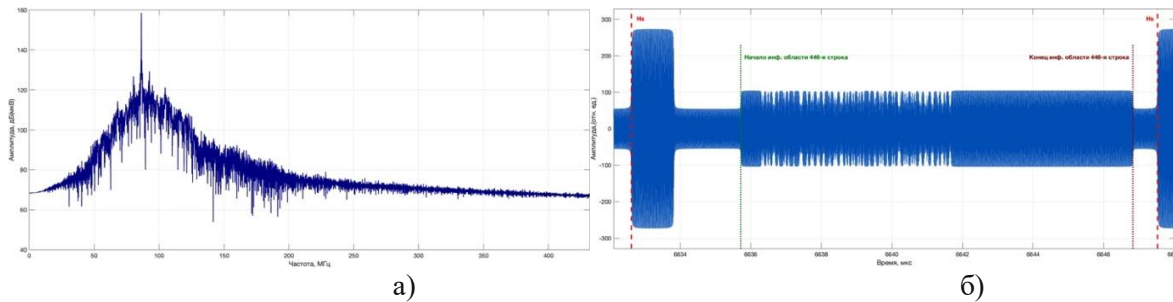


Рисунок 4 – Спектр (а) и осциллограмма (б) сигнала на выходе полосового фильтра

После фильтра промежуточной частоты сигнал поступает на видеодетектор. Огибающая рассчитывается на основе преобразования Гильберта, затем фильтруется низкочастотным фильтром для выделения компоненты, соответствующей изменению яркости изображения. Дискретизация выполняется с частотой 4 ГГц, что обеспечивает достаточную временную детализацию для последующей реконструкции строки.

Для восстановления изображения цифровой сигнал нормируется в диапазоне $[0; 1]$:

$$u_{norm}[n] = \frac{u_c[n] - \min(u_c)}{\max(u_c) - \min(u_c)}, \quad (5)$$

где $u_{norm}[n]$ – нормализованный цифровой видеосигнал в диапазоне;

$u_c[n]$ – отсчеты видеосигнала после цифровой обработки (фильтрации скользящим средним);

$\min(u_c)$ – минимальное значение амплитуды сигнала на анализируемом интервале (уровень «черного» или фоновый шум);

$\max(u_c)$ – максимальное значение амплитуды сигнала (уровень «белого» или пиковое значение импульса).

Далее выполняется детектирование фронтов строчных синхроимпульсов. Порог выбирается адаптивно, а интервалы между найденными фронтами проверяются по ожидаемой длительности строки. При пропусках, вызванных шумовыми выбросами или замираниями сигнала, положение строк восстанавливается по расчетному шагу, соответствующему таймингам VGA.

После определения начала строк выделяются активные участки видеосигнала. Каждый участок интерполируется на равномерную сетку, число отсчетов которой равно горизонтальному разрешению изображения. В результате формируется полутоновая матрица кадра, яркость элементов которой

пропорциональна амплитуде восстановленного видеосигнала. Для повышения разборчивости текста дополнительно применяются адаптивная бинаризация и морфологическая обработка.

На рисунке 5 приведены фрагменты изображений, восстановленных при расстоянии 1 м и различных значениях RBW.

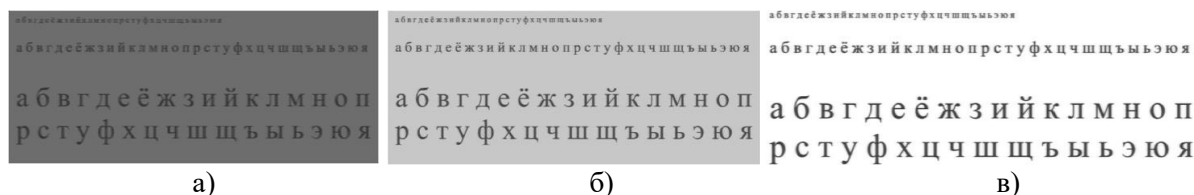


Рисунок 5 – Фрагменты тестовых изображений, восстановленных по результатам перехвата ПЭМИ на расстоянии 1 м, при различных полосах пропускания полосового фильтра приемного устройства: $RBW = 40$ МГц (а), $RBW = 86,4$ МГц (б), $RBW = 344$ МГц (в)

Полученные изображения показывают, что при малой RBW сглаживаются фронты видеосигнала, частично заполняются межсимвольные интервалы и ухудшается устойчивость контуров к пороговой обработке. При увеличении масштаба букв влияние ослабляется, поскольку штрихи занимают большее число пикселей. Цифровая обработка позволяет частично улучшить качество восстановленного изображения, однако не компенсирует потери высокочастотной информации при чрезмерно узкой полосе приемного тракта.

Для количественной оценки качества восстановления используется отношение сигнал/шум изображения, рассчитываемое по статистикам яркости пикселей текста и фона:

$$SNR = 20 \cdot \log_{10} \left((\bar{U}_{\text{бел}} - \bar{U}_{\text{черн}}) / \sqrt{\frac{\sigma_{\text{бел}}^2 + \sigma_{\text{черн}}^2}{2}} \right), \quad (6)$$

где $\bar{U}_{\text{бел}}$ и $\bar{U}_{\text{черн}}$ – средние значения яркости пикселей фона и текста; $\sigma_{\text{бел}}$ и $\sigma_{\text{черн}}$ – среднеквадратические отклонения яркости в соответствующих областях.

Для выбора рационального значения RBW рассчитаны зависимости SNR от отношения RBW/f_n для расстояний 1, 5, 10 и 15 м (рисунок 6а).

Установлено, что максимальные значения SNR достигаются при $RBW \approx 0,7 \cdot f_n$. Дальнейшее расширение полосы не дает заметного прироста полезного сигнала.

Повышение SNR возможно также за счет накопления и усреднения кадров. При некоррелированных шумах выигрыш от усреднения N кадров определяется выражением:

$$SNR_N = SNR + 10 \log_{10} N, N = F_k \cdot T_a, \quad (7)$$

где F_k – частота обновления кадров; T_a – время накопления.

Экспериментальные исследования показывают, что при $SNR \geq 15$ дБ вероятность распознавания текстовых символов приближается к 100% [1]. Следовательно, для обеспечения надежного распознавания необходимо обеспечить условие $SNR_N \geq 15$ дБ.

Расчетные значения T_a для различных исходных SNR представлены на рисунке 6б.

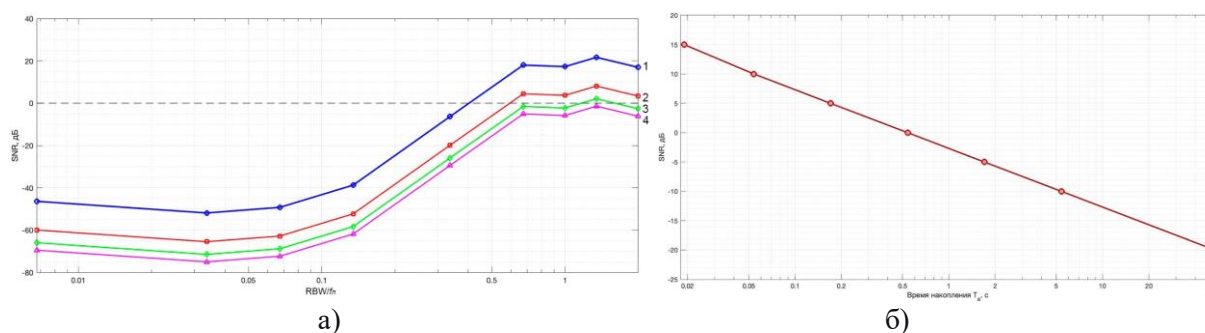


Рисунок 6 – Зависимость SNR от RBW/f_n для различных расстояний перехвата: 1 – 1 м, 2 – 5 м, 3 – 10 м, 4 – 15 м (а); Зависимость минимального времени накопления T_a от исходного SNR (б)

В работе представлена имитационная модель канала перехвата ПЭМИ видеосистем с интерфейсом VGA для исследования влияния полосы пропускания приемного устройства на распознавание текста. Установлено, что максимальное значение SNR достигается при $RBW \approx 0,7 \cdot f_n$, тогда как существенное

снижение вероятности распознавания текста наблюдается при условии $RBW < 0,2 \cdot f_{\Pi}$ в зависимости от масштаба букв. Показано, что при $SNR \geq 15$ дБ вероятность распознавания текстовых символов становится близкой к 100 %. Полученные соотношения позволяют оценивать минимальное время накопления, необходимое для достижения заданного качества распознавания, и могут использоваться при разработке методик оценки возможностей перехвата ПЭМИ СВТ техническими средствами разведки.

Литература

1. Kuhn G. Compromising emanations: eavesdropping risks of computer displays / G. Kuhn // Technical Report UCAM-CL-TR-577. — University of Cambridge, 2005. — 28 p. — URL: <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf> (дата обращения: 30.04.2026).
2. Хорев А. А. Побочные электромагнитные излучения видеосистем средств вычислительной техники / А. А. Хорев // Защита информации. Инсайд. — 2014. — № 1 (55). — С. 52–59.
3. Хорев, А. А. Исследование влияния полосы пропускания приемного устройства средства перехвата ПЭМИ видеосистем, использующих интерфейс VGA, на распознавание текста, выводимого на экран монитора/ А. А. Хорев, О. Р. Лукманова // Защита информации. Инсайд. — 2026. — № 1(127). — С. 22-35.
4. VESA Coordinated Video Timings (CVT) Standard. Revision 1. Draft 6, May 2, 2002 // Video Electronics Standards Association. — 2002. — 46 p. — URL: <https://wiki.geekworn.com/images/5/5c/VESA-Timing-New.pdf> (дата обращения: 30.04.2026).
5. Авдеев В. Б. Методика определения максимальной дальности перехвата побочного электромагнитного излучения при наклонных трассах его распространения / В. Б. Авдеев, А. Н. Картуша // Специальная техника. — 2014. — № 5. — С. 8–16.
6. Анализатор спектра и сигналов R&S®FSW [Электронный ресурс]. — URL: https://spegroup.ru/upload/wikifiles/FSW_broshura.pdf (дата обращения: 30.04.2026).
7. Антенны активные всенаправленные R&S HE600 : руководство по эксплуатации [Электронный ресурс]. — URL: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/HE600-brief-description2024-2025.pdf (дата обращения: 30.04.2026).

SIMULATION MODEL OF THE VGA INTERFACE COMPROMISING EMANATIONS INTERCEPTION CHANNEL FOR STUDYING THE EFFECT OF RECEIVER BANDWIDTH ON TEXT RECOGNITION

sen.lect. Lukmanova O.R.

National Research University of Electronic Technology

The paper presents a simulation model of the interception channel for compromising electromagnetic emanations from VGA-based video systems, developed in the MATLAB environment. The model includes modules for test image synthesis, VGA signal generation, compromising electromagnetic emanation formation and propagation, receiver simulation, and image reconstruction. The effect of the receiver bandwidth (RBW) on the quality of reconstructed text images is investigated. It is shown that reducing RBW leads to smoothing of the video signal edges, lower contrast, and poorer symbol legibility. It is established that the maximum SNR values are achieved at $RBW \approx 0.7f_p$, while at $SNR \geq 15$ dB the probability of text recognition approaches 100%. The results can be used to assess information leakage threats through the compromising electromagnetic emanation channel.



ЦЕПОЧКА ПОСТАВОК В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: КАК ПОДРЯДЧИКИ СТАНОВЯТСЯ ТОЧКОЙ ВХОДА ДЛЯ АТАК

студ. Львов К.А., проф. Душкин А.В.

Национальный исследовательский университет «МИЭТ»

Современные организации всё чаще полагаются на внешних подрядчиков для разработки, сопровождения и эксплуатации информационных систем, что приводит к расширению границ доверия и формированию сложных цепочек поставок. В такой среде компрометация одного участника может представлять серьёзную угрозу безопасности всей экосистемы. В данной работе рассматривается роль подрядчиков как потенциальных точек входа для кибератак в контексте цепочки поставок. В исследовании анализируются типичные векторы атак, включая компрометацию учётных данных, использование каналов удалённого доступа и внедрение вредоносного кода в процессы разработки и распространения программного обеспечения. Особое внимание уделяется реальным инцидентам, демонстрирующим эффективность атак на цепочки поставок и их системное влияние. Для улучшения оценки рисков в работе предлагаются количественные модели, учитывающие такие факторы, как вероятность угрозы, уровень уязвимости, права доступа и потенциальный ущерб. Вводится адаптивный подход к управлению доступом на основе доверия, позволяющий динамически корректировать привилегии подрядчиков в зависимости от их профиля риска. Техническая часть исследует современные архитектуры и средства обеспечения безопасности, включая управление привилегированным доступом (PAM), доступ к сети с нулевым доверием (ZTNA), защищённые CI/CD-конвейеры и аналитику поведения пользователей и сущностей (UEBA). Эти механизмы рассматриваются как часть комплексной многоуровневой стратегии защиты. Результаты подчеркивают необходимость перехода от моделей безопасности, основанных на периметре, к распределённым подходам с учётом доверия. В заключении отмечается, что эффективное снижение рисков цепочки поставок требует интеграции аналитических моделей, технических средств защиты и организационных мер среди всех участников цифровой экосистемы.

Цифровая трансформация и активное развитие аутсорсинга ИТ-услуг привели к тому, что современные организации перестали существовать в изолированном контуре. Информационные процессы выходят за пределы одной компании и включают множество внешних участников, среди которых подрядчики, поставщики программного обеспечения, облачные провайдеры и интеграторы. В этих условиях границы доверия размываются, а традиционные модели защиты, ориентированные на периметр, теряют свою эффективность. Всё чаще злоумышленники используют не прямые атаки на целевую организацию, а косвенные пути – через менее защищённые элементы цепочки поставок.

Цепочка поставок в контексте информационной безопасности представляет собой совокупность всех участников, вовлечённых в процессы создания, поставки, внедрения и поддержки информационных систем. Каждый из этих участников может обладать доступом к критически важным ресурсам, включая исходный код, инфраструктуру, учетные данные и каналы обмена информацией. Такая взаимосвязанность создаёт дополнительные риски, поскольку компрометация одного звена способна привести к каскадным последствиям для всех участников.

Для выполнения своих задач подрядчики получают доступ к внутренним системам заказчика, зачастую на уровне, сопоставимом с доступом штатных сотрудников. При этом контроль за их деятельностью, как правило, ограничен, а уровень зрелости процессов информационной безопасности может существенно отличаться от требований заказчика. Это делает подрядчиков одной из наиболее уязвимых точек в архитектуре безопасности.

Расширение доверенной зоны является одной из ключевых причин роста рисков. Организации вынуждены предоставлять доступы, которые часто оказываются избыточными или сохраняются дольше необходимого. На практике это приводит к формированию так называемого «наследуемого доступа», когда учетные записи продолжают существовать после завершения работ или смены персонала подрядчика.

С аналитической точки зрения, риски цепочки поставок можно рассматривать как произведение вероятности компрометации подрядчика на уровень доверия, предоставленного ему заказчиком. При этом даже относительно низкая вероятность компрометации может приводить к высоким совокупным рискам при наличии широких прав доступа. Это объясняет, почему атаки через подрядчиков становятся всё более привлекательными, так как злоумышленник инвестирует усилия в более слабое звено, получая доступ к более защищённой инфраструктуре.

Одним из наиболее распространённых является компрометация учетных данных подрядчика, после чего злоумышленник получает легитимный доступ к инфраструктуре и может незаметно перемещаться внутри

сети. В таких сценариях традиционные средства защиты, ориентированные на обнаружение внешнего вторжения, оказываются малоэффективными.

Не менее значимым вектором является компрометация процессов разработки и поставки программного обеспечения. Внедрение вредоносного кода на этапе сборки или обновления приводит к тому, что он распространяется как часть доверенного продукта. Это существенно усложняет обнаружение атаки и увеличивает её масштаб. Подобные инциденты демонстрируют, что доверие к поставщику программного обеспечения становится критическим фактором безопасности.

Каналы удалённого доступа, используемые подрядчиками для администрирования систем, также представляют собой значительную угрозу. VPN, RDP и сервисные учетные записи часто обладают расширенными привилегиями и при недостаточном контроле превращаются в прямой канал проникновения. Дополнительную сложность создаёт то, что такие подключения часто рассматриваются как легитимные и не вызывают подозрений у систем мониторинга.

Социальная инженерия усиливает указанные риски. Подрядчики, взаимодействующие с несколькими организациями, обладают более широкой поверхностью атаки и чаще становятся целью фишинговых кампаний. В результате злоумышленник может получить доступ сразу к нескольким инфраструктурам через одну компрометированную учетную запись.

Последствия атак через цепочку поставок носят системный характер. Помимо прямых потерь, связанных с утечками данных и нарушением работы сервисов, организации сталкиваются с каскадными эффектами, включая компрометацию клиентов и партнёров. Это превращает локальный инцидент в масштабный кризис, затрагивающий целые отрасли.

В этих условиях возникает необходимость перехода от реактивной модели безопасности к проактивной. Одним из ключевых направлений является формализация модели доверия. Организациям необходимо явно определять, какие субъекты и на каких условиях получают доступ к ресурсам, а также регулярно пересматривать эти решения. Концепция Zero Trust становится логическим развитием данного подхода, предполагая отказ от доверия по умолчанию и необходимость постоянной проверки всех участников взаимодействия.

С практической точки зрения это означает внедрение механизмов строгой аутентификации и авторизации, сегментации инфраструктуры и изоляции подрядчиков. Особую роль играет динамическое управление доступом, при котором права предоставляются на ограниченное время и автоматически отзываются после завершения задач. Такой подход позволяет существенно снизить риск злоупотребления учетными данными.

Аналитически важным является внедрение метрик оценки рисков подрядчиков. К таким метрикам можно отнести уровень привилегий, частоту доступа, степень интеграции с внутренними системами и зрелость процессов информационной безопасности подрядной организации. Формирование интегрального показателя риска позволяет приоритизировать меры защиты и сосредоточить усилия на наиболее критичных направлениях.

Дополнительным направлением является развитие процессов мониторинга и корреляции событий. Поведенческий анализ действий подрядчиков позволяет выявлять отклонения от нормальной активности, что особенно важно в условиях использования легитимных учетных записей. В этом контексте эффективными являются подходы, основанные на анализе аномалий и построении профилей поведения пользователей.

Организационные меры также играют ключевую роль. Включение требований информационной безопасности в договоры с подрядчиками, проведение регулярных аудитов и обучение персонала позволяют повысить общий уровень защищённости цепочки поставок. Важно отметить, что безопасность в данном случае становится не только технической, но и управленческой задачей.

Отдельное внимание следует уделять безопасности процессов разработки и поставки программного обеспечения. Внедрение практик DevSecOps, контроль зависимостей и защита инфраструктуры сборки позволяют снизить вероятность внедрения вредоносного кода. В условиях роста количества атак на цепочки поставок это направление приобретает стратегическое значение.

Таким образом, цепочка поставок становится одним из ключевых факторов риска в современной информационной безопасности. Подрядчики, являясь необходимым элементом цифровой экосистемы, одновременно выступают потенциальной точкой входа для атак. Эффективное противодействие этим угрозам возможно только при условии комплексного подхода, включающего аналитическую оценку рисков,

внедрение современных архитектур безопасности и развитие процессов взаимодействия с внешними участниками.

Практика последних лет подтверждает, что атаки через цепочку поставок перестали быть теоретической угрозой. Один из наиболее показательных случаев – инцидент с SolarWinds, в рамках которого злоумышленники внедрили вредоносный код в процесс сборки программного обеспечения Orion. Компрометированное обновление было распространено среди тысяч клиентов, включая государственные структуры и крупные корпорации. Ключевой особенностью атаки стало использование доверенного канала обновлений, что позволило обойти традиционные механизмы защиты.

Другим показательным примером является атака на 3CX, где вредоносный компонент был внедрён в десктопное приложение через компрометацию цепочки разработки. В данном случае злоумышленники использовали доверие к поставщику ПО для доставки вредоносной нагрузки конечным пользователям. Аналогичные сценарии наблюдались и в инцидентах, связанных с компрометацией поставщиков идентификационных сервисов, что позволяло атакующим получать доступ к инфраструктурам клиентов.

Анализ этих кейсов позволяет выделить несколько устойчивых закономерностей: во-первых, атака осуществляется на менее защищённое звено; во-вторых, используется доверенный канал взаимодействия; в-третьих, вредоносная активность маскируется под легитимную. Эти факторы существенно усложняют обнаружение и увеличивают время присутствия злоумышленника в системе.

Переход к количественной оценке рисков позволяет уйти от субъективных экспертных суждений и обосновывать управленческие решения в области информационной безопасности. В контексте взаимодействия с подрядчиками это особенно важно, поскольку риск формируется не только внутренними факторами, но и характеристиками внешних организаций. [2]

Базовая модель риска традиционно представляется как произведение вероятности реализации угрозы на величину ущерба:

$$R = P \times I,$$

где:

P – вероятность компрометации подрядчика;

I – ожидаемый ущерб (финансовый, репутационный, операционный).

Однако для практического применения данную модель необходимо декомпозировать. В контексте цепочки поставок целесообразно учитывать следующие факторы:

$$R = (T \times V \times A) \times I,$$

где:

T – вероятность возникновения угрозы (например, вероятность атаки на подрядчика) ;

V – уровень уязвимости подрядной организации (зрелость ИБ, наличие защитных мер) ;

A – уровень доступа подрядчика к системам заказчика (Access Level) ;

I – потенциальный ущерб.

Ключевым отличием этой модели является введение параметра A , который отражает степень доверия. Даже при низкой уязвимости подрядчика высокий уровень доступа можеткратно увеличивать риск.

Для более точной оценки может применяться подход, близкий к методологии FAIR (Factor Analysis of Information Risk), где риск выражается через частоту событий и величину потерь:

$$R = LEF \times LM,$$

где:

LEF (Loss Event Frequency) – частота реализации событий потерь;

LM (Loss Magnitude) – величина потерь.

При этом:

$$LEF = TEF \times Vuln,$$

где:

TEF – частота угроз (например, частота атак на подрядчиков данного типа);

Vuln – вероятность успешной реализации атаки.

Практическая интерпретация данной модели позволяет учитывать статистику атак по отрасли и уровень защищённости конкретного подрядчика.

Дополнительно может вводиться интегральный показатель доверия подрядчику:

$$Trust = w_1 \cdot S + w_2 \cdot C + w_3 \cdot M + w_4 \cdot H,$$

где:

S – зрелость процессов ИБ (security maturity) ;

С – соответствие стандартам (compliance) ;

М – уровень мониторинга и реагирования;

Н – история инцидентов;

w – весовые коэффициенты.

Данный показатель может использоваться для динамического управления доступами:

$$A = f(Trust),$$

то есть уровень доступа подрядчика должен зависеть от его текущего профиля риска.

На практике это позволяет реализовать следующие подходы:

- снижение прав доступа при ухудшении показателей подрядчика;
- приоритизация аудитов;
- обоснование инвестиций в защиту конкретных направлений.

Таким образом, количественные модели позволяют перейти от статической модели доверия к адаптивной, где уровень риска и доступов постоянно пересчитывается.

Современная защита от атак через подрядчиков требует не точечных решений, а построения целостной архитектуры, в которой каждый компонент компенсирует слабости других.

Ключевую роль играет управление привилегированным доступом (PAM). Такие системы обеспечивают централизованный контроль учетных записей подрядчиков, включая:

- выдачу временных учетных данных (Just-in-Time);
- изоляцию сессий;
- запись и аудит действий;
- предотвращение использования постоянных привилегированных учетных записей.

Практически это означает, что подрядчик никогда не обладает «постоянным» доступом, а получает его только на время выполнения задачи, с полной трассировкой действий.

Следующим важным элементом является переход от классических VPN к моделям Zero Trust Network Access (ZTNA). В отличие от VPN, предоставляющего сетевой доступ, ZTNA реализует доступ на уровне приложений с учётом контекста:

- устройства;
- геолокации;
- времени;
- поведения пользователя.

Это позволяет существенно сократить поверхность атаки и исключить горизонтальное перемещение внутри сети.

Сегментация и микросегментация инфраструктуры усиливают данный подход. Подрядчики должны работать в изолированных сегментах, не имея прямого доступа к критическим системам, что позволяет ограничивать масштаб атаки даже при компрометации учетной записи.

Особое внимание необходимо уделять безопасности цепочки разработки (CI/CD). Основные меры включают:

- контроль целостности пайплайнов (защита от несанкционированных изменений);
- обязательную подпись артефактов и проверку на стороне потребителя;
- использование Software Composition Analysis (SCA) для контроля зависимостей;
- изоляцию сред сборки (build environments);
- контроль доступа к репозиториям и системам сборки.

Эти меры направлены на предотвращение сценариев, при которых вредоносный код внедряется на этапе разработки и распространяется как легитимное обновление.

Мониторинг и обнаружение угроз должны строиться с учётом того, что злоумышленник может использовать легитимные учетные записи. В этом контексте особую роль играет поведенческая аналитика (UEBA), которая позволяет:

- выявлять отклонения от нормального поведения;
- обнаруживать аномальные паттерны доступа;
- реагировать на подозрительную активность в реальном времени.

UEBA дополняется системами корреляции событий (SIEM), объединяющими данные из различных источников: сетевых устройств, систем аутентификации, приложений.

Дополнительным уровнем защиты является управление идентификацией и доступом (IAM), включающее:

- обязательную многофакторную аутентификацию (MFA);
- федерацию идентификаций;
- централизованное управление учетными записями подрядчиков.

Криптографические меры также играют важную роль. Использование аппаратных модулей безопасности (HSM) позволяет защитить ключи и критические операции, снижая риск компрометации.

В совокупности данные меры формируют многоуровневую архитектуру защиты, в которой компрометация одного элемента не приводит к полной потере контроля. Такой подход соответствует современным принципам построения защищённых систем и позволяет существенно снизить риски, связанные с подрядными организациями.

Литература

1. ГОСТ Р 59215-2020. Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 3. Рекомендации по обеспечению безопасности цепи поставок ИКТ. – М.: Стандартиформ, 2020.с.
2. Boyens J., Smith A., Bartol N. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. – Gaithersburg: NIST, 2024. – SP 800-161r1.

SUPPLY CHAIN IN INFORMATION SECURITY: HOW CONTRACTORS BECOME AN ENTRY POINT FOR ATTACKS

stud. Lvov K.A., prof. Dushkin A.V.

National Research University of Electronic Technology

Modern organizations increasingly rely on external contractors for the development, maintenance, and operation of information systems, which leads to the expansion of trust boundaries and the formation of complex supply chains. In such an environment, the compromise of a single participant can pose significant risks to the security of the entire ecosystem. This paper examines the role of contractors as potential entry points for cyberattacks within the supply chain context. The study analyzes typical attack vectors, including credential compromise, exploitation of remote access channels, and the insertion of malicious code into software development and distribution processes. Particular attention is paid to real-world incidents that demonstrate the effectiveness of supply chain attacks and their systemic impact. To improve risk assessment, the paper proposes quantitative models that incorporate factors such as threat likelihood, vulnerability level, access privileges, and potential impact. An adaptive trust-based approach to access control is introduced, enabling dynamic adjustment of contractor privileges based on their risk profile. The technical section explores modern security architectures and controls, including Privileged Access Management (PAM), Zero Trust Network Access (ZTNA), secure CI/CD pipelines, and User and Entity Behavior Analytics (UEBA). These mechanisms are considered as part of a comprehensive, multi-layered defense strategy. The results highlight the need for a shift from perimeter-based security models to distributed and trust-aware approaches. The paper concludes that effective mitigation of supply chain risks requires the integration of analytical models, technical controls, and organizational measures across all participants in the digital ecosystem.



ОЦЕНКА ВОЗМОЖНОСТИ АВТОМАТИЗАЦИИ КОНТРОЛЯ ФУНКЦИОНИРОВАНИЯ ОТДЕЛЬНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

асп. Минкин А.Д.

Национальный исследовательский университет «МИЭТ»

В статье рассматривается проблема обеспечения работоспособности средств защиты информации (СЗИ) в автоматизированных системах управления технологическими процессами (АСУ ТП). Целью работы является анализ и оценка возможности автоматизации процессов контроля функционирования отдельных СЗИ. В основу исследования положен подход, при котором работоспособность СЗИ определяется через совокупность признаков неработоспособности, выявленных в ходе анализа архитектуры и особенностей эксплуатации указанных средств. В работе приведены результаты сопоставления показателей неработоспособности и указывающих на них признаков, а также детально описаны способы выявления данных признаков. Проведен анализ применимости стандартных утилит (ping, telnet, systemctl) и специализированных программных интерфейсов для автоматического мониторинга состояния компонентов защиты. Полученные результаты могут служить основой для разработки централизованного комплекса контроля функционирования системы обеспечения информационной безопасности.

В условиях возрастающей сложности киберугроз обеспечение непрерывности и корректности функционирования средств защиты информации (СЗИ) автоматизированных систем управления технологическими процессами (АСУ ТП) является критически важной задачей. Нарушение работы любого компонента системы обеспечения информационной безопасности (СОИБ) может привести к снижению уровня защищенности объекта. В связи с этим актуальной становится задача перехода от периодического ручного контроля состояния СЗИ к непрерывному автоматизированному мониторингу их работоспособности.

В границы, рассмотренные в данной статье, включены три типа СЗИ, широко применяемых для защиты АСУ ТП: программные изделия Kaspersky Endpoint Security (KES) совместно с сервером администрирования Kaspersky Security Center (KSC), программно-аппаратный комплекс UserGate, а также система обнаружения компьютерных атак ViPNet Intrusion Detection System (IDS). Под работоспособностью СЗИ в рамках работы понимается штатное функционирование всех компонентов перечисленных средств и реализация ими предусмотренных мер безопасности.

Целью данной статьи является оценка возможности автоматизации выявления неработоспособности СЗИ. Для ее достижения был проведен анализ архитектуры, особенностей функционирования и принципов эксплуатации рассматриваемых изделий, по результатам которого сформирован перечень показателей неработоспособности, указывающих на них признаков и способов их выявления. При определении способов выявления в приоритетном порядке рассматривались встроенные функции компонентов СЗИ, а при их отсутствии – возможности системного и прикладного программного обеспечения среды функционирования.

Описание подходов к проведению контроля функционирования СЗИ

Оценку работоспособности СЗИ предлагается проводить путем анализа совокупности признаков неработоспособности СЗИ (возможных причин нарушения в работе СЗИ), при этом СЗИ признается работоспособным, если не выявлен ни один из признаков его неработоспособности, в противном случае СЗИ признается неработоспособным.

Для определения перечня признаков неработоспособности СЗИ проведен анализ архитектуры, особенностей функционирования, а также принципов эксплуатации и управления рассматриваемых СЗИ, по результатам которого сформирован перечень показателей неработоспособности СЗИ (проявлений проблем в работе СЗИ) и указывающих на них признаков неработоспособности. Для каждого из сформированных признаков неработоспособности СЗИ определен способ его выявления (при наличии технической возможности).

В качестве исходных данных при определении показателей неработоспособности СЗИ использовались сведения о возможных видах отказов, полученные в ходе эксплуатации СЗИ.

При формировании перечня показателей неработоспособности СЗИ и указывающих на них признаков неработоспособности приняты следующие условия, ограничения и допущения:

- не рассматривались действия (санкционированные, несанкционированные, случайные, преднамеренные) обслуживающего и эксплуатационного персонала, а также иных лиц по вмешательству в работу СЗИ (включая изменение параметров конфигурации, управление работой компонентов СЗИ и т.д.);
- в качестве признаков неработоспособности СЗИ рассматривались верхнеуровневые причины, непосредственно указывающие на проявление проблем в работе СЗИ, без рассмотрения всей последовательности возможных причин.

При определении способов выявления признаков неработоспособности СЗИ приняты следующие условия, ограничения и допущения:

- в приоритетном порядке рассматривались встроенные функции и возможности компонентов СЗИ, а при их отсутствии – возможности системного и прикладного программного обеспечения (ПО), обеспечивающего среду функционирования компонентов СЗИ;
- не рассматривалось использование интерфейсов Application Programming Interface (API) компонентов СЗИ, для которых производителем не представлена документация по его применению и отсутствует техническая поддержка (возможность консультаций).

Показатели и признаки неработоспособности СЗИ

Исходя из результатов анализа архитектуры, особенностей функционирования, а также принципов эксплуатации и управления вышеописанных программных изделий сформирован перечень показателей неработоспособности СЗИ и указывающих на них признаков неработоспособности.

Для СЗИ KES и KSC были определены показатели неработоспособности (представлены в таблице 1), а также следующие признаки неработоспособности:

1. АРМ или сервер выключен;
2. служба (сервис) СУБД не функционирует (не запущена);
3. ошибки в алгоритме работы программных средств СУБД;
4. служба (сервис) KES не функционирует (не запущена);
5. ошибки в алгоритме работы программных средств KES;
6. служба (сервис) KSC не функционирует (не запущена);
7. ошибки в алгоритме работы программных средств KES;
8. отсутствие действующей лицензии;
9. отсутствие сетевой доступности.

Сопоставление показателей неработоспособности KES и KSC с указывающими на них признаками неработоспособности в виде матрицы приведено в таблице 1.

Таблица 1

Матрица показателей неработоспособности СЗИ (KES и KSC)

№	Показатель неработоспособности	Признаки неработоспособности								
		1	2	3	4	5	6	7	8	9
1	KES не функционирует (не запущен)	+			+	+				
2	Не функционирует один или несколько компонентов KES	+			+	+			+	
3	В KES не выполняются настроенные задачи	+			+	+			+	
4	В KES используется неактуальная база данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+	+	+	+	+	+
5	В журналах регистрации KES не осуществляется регистрация событий безопасности	+			+	+			+	
6	Не запускается веб-консоль администрирования KSC							+		
7	На сервере администрирования KSC не осуществляется обслуживание базы данных		+	+			+	+		
8	Нарушение или прекращение взаимодействия между сервером администрирования KSC и KES	+	+	+	+	+	+	+		+
9	На сервере администрирования KSC используется неактуальная база данных		+	+			+	+		+

№	Показатель неработоспособности	Признаки неработоспособности								
		1	2	3	4	5	6	7	8	9
	признаков вредоносных компьютерных программ (вирусов)									
10	На сервере администрирования KSC не осуществляется выполнение резервного копирования данных		+	+			+	+		
11	В журналах регистрации сервера администрирования KSC не осуществляется регистрация событий безопасности						+	+		
12	На сервере администрирования KSC используется некорректная дата и (или) время							+		
13	С сервера администрирования KSC не осуществляется передача событий безопасности в SIEM		+	+			+	+		
14	Сервером администрирования KSC не осуществляется рассылка отчетов		+	+			+	+		+

Для СЗИ UserGate также были определены показатели неработоспособности (представлены в таблице 2), а также следующие признаки неработоспособности:

1. нарушение или прекращение функционирования компонентов аппаратной (виртуальной) платформы;
2. ошибки в алгоритме работы программных средств UserGate;
3. отсутствие действующей лицензии;
4. отсутствие сетевой доступности.

Сопоставление показателей неработоспособности UserGate с указывающими на них признаками неработоспособности в виде матрицы приведено в таблице 2.

Таблица 2

Матрица показателей неработоспособности СЗИ (UserGate)

№	Показатель неработоспособности	Признаки			
		1	2	3	4
1	Нарушение или прекращение функционирования механизма кластеризации UserGate	+	+		+
2	Нарушение или прекращение функционирования одного или обоих узлов кластера UserGate	+	+		
3	Отсутствует доступ к интерфейсам управления кластера UserGate	+	+		+
4	Нарушение и (или) прекращение функционирования одного или нескольких модулей кластера UserGate, предусмотренных к использованию (модуль МЭ, модуль COB, модуль DOS, модуль защиты АСУ ТП и т.д.)	+	+	+	
5	В журналах регистрации UserGate не осуществляется регистрация событий безопасности	+	+		
6	С кластера UserGate не осуществляется передача событий безопасности в SIEM	+	+		+
7	Отсутствует доступ к интерфейсам управления UserGate MC (интерфейсу командной строки, веб-интерфейсу управления)	+	+		+
8	Отсутствует возможность изменения параметров конфигурации кластера UserGate UTM с использованием UserGate MC	+	+		
9	Нарушение или прекращение взаимодействия между кластером UserGate UTM и UserGate MC	+	+		+

Для СЗИ ViPNet IDS были определены показатели неработоспособности (представлены в таблице 3), а также следующие признаки неработоспособности:

1. нарушение или прекращение функционирования компонентов платформы ViPNet IDS NS;
2. нарушение или прекращение функционирования компонентов платформы ViPNet IDS MC;
3. ошибки в алгоритме работы программных средств сенсора ViPNet IDS NS;
4. ошибки в алгоритме работы программных средств сервера управления ViPNet IDS MC
5. отсутствие действующей лицензии;
6. отсутствие сетевой доступности.

Сопоставление показателей неработоспособности VipNet с указывающими на них признаками неработоспособности в виде матрицы приведено в таблице 3.

Таблица 3

Матрица показателей неработоспособности СЗИ (ViPNet)

№	Показатель неработоспособности	Признаки					
		1	2	3	4	5	6
1	Отсутствует доступ к интерфейсам управления сенсора ViPNet IDS NS	+		+			+
2	Нарушение и (или) прекращения функционирования одного или нескольких модулей сенсора ViPNet IDS NS			+			
3	На сенсоре ViPNet IDS NS используется некорректная дата и (или) время			+			+
4	В журналах регистрации сенсора ViPNet IDS NS не осуществляется регистрация событий безопасности	+		+			
5	Сенсором ViPNet IDS NS не осуществляется отправка оповещений о событиях безопасности по электронной почте	+		+			+
6	Нарушение или прекращение взаимодействия между сенсором ViPNet IDS NS и сервером управления ViPNet IDS MC	+	+	+	+		+
7	С сенсора ViPNet IDS NS не осуществляется передача событий безопасности в SIEM	+		+			+
8	Отсутствует доступ к веб-интерфейсу управления сервером управления ViPNet IDS MC		+		+		+
9	Отсутствует доступ к консольному конфигуратору сервера управления ViPNet IDS MC		+		+		

Оценка возможности автоматизации

Следующим этапом в исследовании стало определение способов выявления признаков неработоспособности, определенных на предыдущем шаге, а также оценка возможности автоматизации такого выявления.

В рамках статьи приводится вырезка из полной таблицы оценки возможности автоматизации (по 1 признаку для каждого из рассматриваемых СЗИ). Вырезка представлена в таблице 4.

Таблица 4

Оценка возможности автоматизации

№	Признак неработоспособности	Способ выявления признака	Возможность автоматизации
KES и KSC			
1	Служба (сервис) KES не функционирует (не запущена)	Проверка состояния службы (сервиса) KES на APM или сервере с использованием встроенных механизмов используемой ОС	Автоматизация возможна: проверка с использованием утилиты systemctl
UserGate			
2	Отсутствие действующей лицензии	Проверка статуса лицензии с использованием встроенных механизмов UserGate UTM или UserGate MC	Автоматизация возможна: проверка путем подключения к узлу по SSH и выполнения команды license show
ViPNet IDS			

№	Признак неработоспособности	Способ выявления признака	Возможность автоматизации
3	Ошибки в алгоритме работы программных средств сенсора ViPNet IDS NS	Проверка журналов регистрации сенсора ViPNet IDS NS на наличие записей об ошибках в работе	Автоматизация возможна, анализ записей регистрации событий сенсора ViPNet IDS NS в SIEM

На основе анализа таблиц неработоспособности установлено, что для большинства признаков технически реализуема автоматизация. Вместе с тем выявлен ряд принципиально неавтоматизируемых проверок, обусловленных отсутствием в конкретных СЗИ требуемых механизмов. Полученные результаты будут использованы при проектировании централизованного комплекса контроля функционирования СЗИ.

Литература

1. Еремеев М. А. Взаимосвязь информационной безопасности и надежности в автоматизированных системах управления технологическими процессами /М. А. Еремеев, А. Г. Линючев // VII Международная научно-практическая конференция «Инновационные аспекты развития науки и техники». — 2021. — С. 15-25. — URL: <https://cyberleninka.ru/article/n/relation-between-information-security-and-reliability-in-industrial-control-systems-for-technological-processes/viewer> (дата обращения: 05.04.2026).
2. Скрипова В. Р. Обзор решений для оптимизации системы управления комплексом защиты объекта / В. Р. Скрипова, К. А. Аксенов // Инженерный вестник Дона. — 2025. — № 3. — URL: <https://cyberleninka.ru/article/n/obzor-resheniy-dlya-optimizatsii-sistemy-upravleniya-kompleksom-zaschity-obekta> (дата обращения: 01.05.2026).

ASSESSING THE FEASIBILITY OF AUTOMATING THE MONITORING OF THE FUNCTIONING OF INDIVIDUAL INFORMATION SECURITY TOOLS

stud. A.D. Minkin

National Research University MIET

The article examines the problem of ensuring the operability of information security tools in automated process control systems (APCS). The aim of the work is to analyze and assess the feasibility of automating the processes for monitoring the functioning of individual security tools. The study is based on an approach in which the operability of information security tools is determined through a set inoperability indicators identified during the analysis of the architecture and operational characteristics of these tools. The paper presents the results of comparing inoperability indicators and their corresponding signs, as well as a detailed description of methods for detecting these signs. An analysis is conducted on the applicability of standard utilities (ping, telnet, systemctl) and specialized software interfaces for the automatic monitoring of the state of security components. The obtained results can serve as a basis for the development of a centralized monitoring system for the functioning of the information security system.



ИССЛЕДОВАНИЕ ФРАЗОВОЙ РАЗБОРЧИВОСТИ РЕЧИ В УСЛОВИЯХ ПОМЕХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

проф. Хорев А.А., студ. Моложавцев Е.О.

Национальный исследовательский университет «МИЭТ»

В статье представлены результаты экспериментальных исследований разборчивости речевых сигналов с использованием технологий искусственного интеллекта. В качестве систем автоматизированного распознавания (АСР) были использованы системы «WhisperX-large-v3» и GigaAM-RNNT-v3, а в качестве исходных тестовых речевых сигналов – артикуляционные таблицы фраз. По результатам экспериментальных исследований фразовая разборчивость исходных тестовых речевых сигналов составила для АСР «WhisperX-large-v3» – 99,9%, а для АСР GigaAM-RNNT-v3 – 90,7%. В качестве шумовых сигналов шумовой «речеподобный» сигнал и помеховый сигнал типа «речевой хор». Формирование зашумленных речевых сигналов осуществлялось путем смешения исходных тестовых речевых сигналов с шумом с отношениями сигнал/шум от – 20 до +10 дБ с шагом в 2 дБ. В результате экспериментальных исследований установлено, что АСР «WhisperX-large-v3» по сравнению с АСР «GigaAM-RNNT-v3» обеспечивает более высокую фразовую разборчивость речи при всех видах помех. Для этой АСР фразовая разборчивость выше 20% наблюдается при шумовой «речеподобной» помехе – при отношении сигнал/шум выше минус 6 дБ, для помехи типа «речевой хор» – при отношении сигнал/шум выше минус 2 дБ. При низких отношениях сигнал/шум (менее 2 дБ) фразовая разборчивость речи, полученная АСР, существенно ниже фразовой разборчивости, полученной методом артикуляционных испытаний.

В качестве показателя эффективности защиты акустической речевой информации используется словесная разборчивость речи, под которой понимается относительное количество правильно понятых человеком слов из перехваченного разговора [1].

Учитывая, что целью акустической речевой разведки является получение смыслового содержания перехваченного разговора (то есть не отдельных слов, а связанного текста), для оценки возможностей акустической речевой разведки целесообразно рассмотреть фразовую разборчивость речи.

Одним из основных методов оценки разборчивости речи в условиях помех является метод артикуляционных испытаний [2].

Проведение артикуляционных испытаний является довольно трудоемким и дорогим процессом.

Одним из направлений, существенно снижающих время и стоимость проведения артикуляционных испытаний, является использование технологий искусственного интеллекта.

Цель проводимых исследований – оценить возможность использования технологий искусственного интеллекта для распознавания речи в условиях помех при низких отношениях сигнал/шум.

Проведенный анализ научной литературы показал, что одними из наиболее эффективных систем автоматизированного распознавания русской речи (АСР) являются системы «WhisperX-large-v3» (США) и «GigaAM-RNNT-v3» (Россия) [3, 4, 5].

Исследования разборчивости речи с использованием АСР проводились в три этапа.

На первом этапе проводилась оценка фразовой разборчивости речи при высоких отношениях сигнал/шум.

В качестве исходных тестовых речевых сигналов использовались артикуляционные таблицы фраз [2]. Запись исходных тестовых речевых сигналов проводилась бригадой из 6-ти дикторов (4 мужчины и 2 женщины), не имеющих дефектов речи.

Для проведения оценки распознавания речи на языке программирования Python было разработано специальное программное обеспечение (СПО) и реализовано в облачной среде выполнения Google colab.

Методика проведения исследований заключалась в следующем:

с использованием СПО аудиофайлы с записями таблиц фраз загружались в АСР;

АСР проводила распознавание слов. Результат распознавания записывался в текстовый документ.

Далее с использованием СПО результат приводился к удобной для сравнения форме, фонетически нормализовывался и сравнивался с эталонным текстом, по итогу сравнения рассчитывалось количество правильно распознанных фраз по формуле (1):

$$W_{ik} = N_{ik}/N, \quad (1)$$

где W_k – фразовая разборчивость аудиофайла с записью фраз i -й таблицы, определенная k -м аудитором;

N_{ik} – количество правильно распознанных k -м аудитором фраз в аудиофайле с записью фраз i -й таблицы (фраза считалась правильно понятой, если АСР правильно передавала ее смысл);

N – общее количество фраз в аудиофайле ($N=50$).

Результаты оценки фразовой разборчивости речи, распознанной АСР «GigaAM-RNNT-v3», приведены в таблице 1, а распознанные АСР «WhisperX_large-v3» – в таблице 2.

Таблица 1

Результаты оценки фразовой разборчивости речи, распознанной АСР «GigaAM-RNNT-v3»,
при высоких отношениях сигнал/шум

Диктор	Фразовая разборчивости речи, %				
	1 таблица	2 таблица	3 таблица	4 таблица	5 таблица
1	100	86	76	80	66*
2	98	98	98	96	90
3	94	94	98	86	96
4	98	88	84	82	90
5	-	94	92	82	84
6	90	96	100	94	96
Средняя разборчивость по таблицам	96	92,67	91,33	86,67	87
Средняя разборчивость по таблицам и дикторам	90,7				

*Примечание - паузы для 5 таблицы 1 диктора примерно в 2 раза дольше, чем в остальных аудиозаписях.

Таблица 2

Результаты оценки фразовой разборчивости речи, распознанной АСР «WhisperX_large-v3»
при высоких отношениях сигнал/шум

Диктор	Фразовая разборчивости речи, %				
	1 таблица	2 таблица	3 таблица	4 таблица	5 таблица
1	100	100	100	100	98*
2	100	100	100	100	100
3	100	100	100	100	100
4	100	100	100	100	100
5	-	100	100	100	100
6	100	100	100	100	100
Средняя разборчивость по таблицам	100	100	100	100	99,7
Средняя разборчивость по таблицам и дикторам	99,9				

*Примечание - паузы для 5 таблицы 1 диктора примерно в 2 раза дольше, чем в остальных аудиозаписях.

Анализ данных, представленных в таблицах 1 и 2, показывает, что при высоких отношениях сигнал/шум (практически в отсутствие шумов) фразовая разборчивость для АСР «GigaAM-RNNT-v3» составляет около 91%, а для АСР «WhisperX_large-v3» – близка к 100%.

На втором этапе проводилась оценка фразовой разборчивости зашумленных речевых сигналов.

В качестве шумовых сигналов были выбраны два наиболее эффективных вида помех: шумовой «речеподобный» сигнал и помеховый сигнал типа «речевой хор».

Для формирования помех использовалась ПЭВМ и специальное программное обеспечение Adobe Audition 1.5 [6].

Шумовая «речеподобная» помеха формировалась из «белого» шума путем изменения его огибающей спектра с использованием графического десяти полосового эквалайзера (инструмент «Эффекты» - «Фильтры» - «Графический эквалайзер»).

Помеха типа «речевой хор» была сформирована из смеси речевых сигналов пяти дикторов. В качестве исходных речевых сигналов использовались записи таблиц фраз [2]. При этом при формировании помехи паузы между словами из записей удалялись.

При проведении экспериментальных исследований под отношением сигнал/шум понималось среднее отношение речевой сигнал/шум за весь период воспроизведения диктором артикуляционной таблицы. При этом, при измерении уровня сигнала из аудиофайла с записью исходного тестового речевого сигнала удалялись паузы между словами.

Формирование зашумленных тестовых речевых сигналов осуществлялось путем смешения речевых сигналов (исходных тестовых речевых сигналов с паузами) с помеховыми.

Для оценки разборчивости речи были сформированы аудиофайлы с отношениями сигнал/шум от – 20 до +10 дБ с шагом в 2 дБ.

Результаты оценки фразовой разборчивости речи, распознанной АСР «GigaAM-RNNT-v3», приведены в таблиц 3, а распознанные АСР «WhisperX_large-v3» – в таблице 4.

Таблица 3

Результаты оценки разборчивости зашумленной речи АСР «GigaAM-RNNT-v3»

Отношение сигнал/шум, дБ	Фразовая разборчивости речи, %					
	Шумовая «речеподобная» помеха			Помеха типа «речевой хор»		
	Диктор 2, 1 таблица	Диктор 4, 1 таблица	Средняя разбор- чивость	Диктор 2, 1 таблица	Диктор 4, 1 таблица	Средняя разборчивость
-20	0	0	0	0	0	0
-18	0	0	0	0	0	0
-16	0	0	0	0	0	0
-14	0	0	0	0	0	0
-12	0	0	0	0	0	0
-10	0	0	0	0	0	0
-8	0	0	0	0	0	0
-6	0	0	0	0	0	0
-4	0	24	12	2	0	1
-2	72	32	52	36	4	20
0	80	58	69	76	22	49
2	86	74	80	96	60	78
4	88	84	86	96	84	90
6	90	96	93	96	90	93
8	94	96	95	98	96	97
10	96	96	96	100	100	100

На третьем этапе была проведена оценка фразовой разборчивости зашумленной речи методом артикуляционных испытаний.

Испытания проводились бригадой auditors в составе 8 человек в возрасте от 20 до 23 лет. Все аудиторы не имели дефектов слуха.

Для прослушивания аудиторам предъявлялись аудиофайлы с записями зашумленных речевых сигналов. Для прослушивания зашумленных речевых сигналов использовались ПЭВМ и медиаплеер VLC. Прослушивание сигналов осуществлялось аудиторами через головные наушники AKG K271 MKII, подключаемые к линейному выходу звуковой карты ПЭВМ.

Аудиторы прослушивали аудиофайлы с записью зашумленных тестовых речевых сигналов с отношением сигнал/шум от – 20 до +10 дБ с шагом 2 дБ. Для каждого вида шума прослушивание аудиофайлов начиналось с файла с наименьшим отношением сигнал/шум $q = -20$ дБ и заканчивается аудиофайлом с максимальным значением отношения сигнал/шум $q = +20$ дБ.

После прослушивания каждой фразы аудитор останавливал воспроизведение записи и заносил услышанную фразу в таблицу. При сложности восприятия разрешается аудитор мог отматывать запись назад и повторно прослушивать фразу.

Таблица 4

Результаты оценки разборчивости зашумленной речи АСР «WhisperX_large-v3»

Отношение сигнал/шум, дБ	Фразовая разборчивости речи, %					
	Шумовая «речеподобная» помеха			Помеха типа «речевой хор»		
	Диктор 2, 1 таблица	Диктор 4, 1 таблица	Средняя разбор- чивость	Диктор 2, 1 таблица	Диктор 4, 1 таблица	Средняя разборчивость
-20	0	0	0	0	0	0
-18	0	0	0	0	0	0
-16	0	0	0	0	0	0
-14	0	0	0	0	0	0
-12	0	0	0	0	0	0

-10	0	0	0	0	0	0
-8	16	0	8	0	0	0
-6	34	22	28	0	0	0
-4	56	52	54	12	0	6
-2	78	66	72	58	26	42
0	88	78	83	90	54	72
2	98	92	95	96	84	90
4	100	98	99	98	92	95
6	100	98	99	98	92	95
8	100	100	100	98	94	96
10	100	100	100	98	96	97

В результате обработки результатов распознавания зашумленных фраз для каждого вида помехи и отношения сигнал/шум рассчитывалась фразовая разборчивость речи для каждого аудитора и средняя фразовая разборчивость по группе.

Результаты сравнительной оценки словесной разборчивости зашумленной речи, проведенной с использованием САР, и проведенной методом артикуляционных испытаний с привлечением 8 аудиторов, приведены в таблице 5.

Таблица 5

Результаты сравнительной оценки фразовой разборчивости зашумленной речи, проведенной с использованием САР, и проведенной методом артикуляционных испытаний с привлечением 8 аудиторов

Отношение сигнал/шум, дБ	Фразовая разборчивости речи, %					
	Шумовая «речеподобная» помеха			Помеха типа «речевой хор»		
	«GigaAM-RNNT-v3»	«Whisperx_large-v3»	Артикуляционные испытания	«GigaAM-RNNT-v3»	«Whisperx_large-v3»	Артикуляционные испытания
-20	0	0	0	0	0	0
-18	0	0	0	0	0	0
-16	0	0	0	0	0	0
-14	0	0	0	0	0	0
-12	0	0	4	0	0	0
-10	0	0	16	0	0	0
-8	0	8	32	0	0	2
-6	0	28	50	0	0	17
-4	12	54	67	1	6	46
-2	52	72	79	20	42	74
0	69	83	89	49	72	89
2	80	95	94	78	90	97
4	86	99	97	90	95	99
6	93	99	99	93	95	99
8	95	100	100	97	96	100
10	96	100	100	100	97	100

Анализ данных, представленных в таблицах 3 – 5, показал, что:

- при отношениях сигнал/шум $q \geq 2$ дБ фразовая разборчивость речи, полученная АСР при распознавании речевых сигналов, зашумленных шумовой «речеподобной» помехой, сопоставима с фразовой разборчивости, полученной методом артикуляционных испытаний;
- при низких отношениях сигнал/шум $q \leq 0$ дБ фразовая разборчивость речи, полученная АСР при распознавании речевых сигналов, зашумленных шумовой «речеподобной» помехой, существенно ниже фразовой разборчивости, полученной методом артикуляционных испытаний;
- при отношениях сигнал/шум $q \leq -6$ дБ АСР не способны распознавать зашумленные помехой типа «речевой хор» речевые сигналы, тогда, как при $q = -6$ дБ фразовая разборчивость речи, полученная методом артикуляционных испытаний, составляет 17%;

- по сравнению АСР «GigaAM-RNNT-v3» АСР «WhisperX-large-v3» обеспечивает более высокую фразовую разборчивость речи при всех видах помех;
- при низких отношениях сигнал/шум $q \leq 0$ дБ наиболее эффективной является помеха типа «речевой хор». Например, при отношении сигнал/шум $q \leq -6$ дБ фразовая разборчивость речи полученная АСР «WhisperX-large-v3» для шумовой «речеподобной» помехи составила 28%, а для помехи типа «речевой хор» – 0%.

Следовательно, при отношениях сигнал/шум выше 2 дБ артикуляционные испытания для шумовой «речеподобной» помехи могут проводиться с использованием АСР «WhisperX-large-v3».

Литература

1. Хорев А.А. Оценка возможностей средств акустической (речевой) разведки//Специальная техника. – М.: 2009. – № 4 – С. 49-63.
2. ГОСТ Р 50840-95. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. – Введ. 1997-01-01. – М.: Изд-во стандартов, 1996. – 202 с.
3. Radford A., Kim J.W., Xu T., Brockman G., McLeavey C., Sutskever I. Robust Speech Recognition via Large-Scale Weak Supervision // Proceedings of the 40th International Conference on Machine Learning (ICML 2023). – Honolulu, Hawaii, USA, 2023. – С. 28492-28518.
4. Bain M., Huh J., Han T., Zisserman A. WhisperX: Time-Accurate Speech Transcription of Long-Form Audio// Препринт. – Oxford, 2024. – С. 1-6.
5. Kutsakov A., Maximenko A., Gospodinov G., Bogomolov P., Minkin F. GigaAM: Efficient Self-Supervised Learner for Speech Recognition // Труды конференции Interspeech 2025. – Rotterdam, The Netherlands, 2025. – С. 1-5.
6. Adobe AUDITION 1.5: Руководство пользователя. [Электронный ресурс]. – Режим доступа: <https://www.manualslib.com/manual/1995/Adobe-Audition-1-5.html>.

RESEARCH OF PHRAZAL SPEECH DISCRIMINABILITY IN INTERFERENCE CONDITIONS USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Prof. Horev A.A., stud. Molozhavgsev E.O.

National Research University of Electronic Technology

The article presents the results of experimental studies of speech signal intelligibility using artificial intelligence technologies. The WhisperX-large-v3 and GigaAM-RNNT-v3 automated speech recognition systems (ASR) were used, and articulation tables of phrases were used as the original test speech signals. According to the results of the experimental studies, the phrase intelligibility of the original test speech signals was 99.9% for the WhisperX-large-v3 ASR, and 90.7% for the GigaAM-RNNT-v3 ASR. The noise signals were a speech-like noise signal and a speech choir interference signal. The noisy speech signals were formed by mixing the original test speech signals with noise with a signal-to-noise ratio from -20 to +10 dB in 2 dB increments. Experimental studies have shown that the WhisperX-large-v3 automated speech recognition system, compared to the GigaAM-RNNT-v3 automated speech recognition system, provides superior phrase intelligibility across all types of interference. This automated speech recognition system achieves phrase intelligibility above 20% with speech-like noise (at a signal-to-noise ratio above minus 6 dB), and with chorus-type interference (at a signal-to-noise ratio above minus 2 dB). At low signal-to-noise ratios (less than 2 dB), the phrase intelligibility obtained with the automated speech recognition system is significantly lower than that obtained through articulation testing



ИССЛЕДОВАНИЕ СЛОВЕСНОЙ РАЗБОРЧИВОСТИ РЕЧИ В УСЛОВИЯХ ПОМЕХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

проф. Хорев А.А., студ. Моложавцев Е.О.

Национальный исследовательский университет «МИЭТ»

В статье представлены результаты экспериментальных исследований разборчивости речевых сигналов с использованием технологий искусственного интеллекта. В качестве систем автоматизированного распознавания (АСР) были использованы системы «WhisperX-large-v3» и GigaAM-RNNT-v3, а в качестве исходных тестовых речевых сигналов – артикуляционные таблицы односложных слов. По результатам экспериментальных исследований словесная разборчивость исходных тестовых речевых сигналов составила для АСР «WhisperX-large-v3» – 99,5%, а для АСР GigaAM-RNNT-v3 – 94,2%. Формирование зашумленных речевых сигналов осуществлялось путем смещения исходных тестовых речевых сигналов с «белым» шумом с отношениями сигнал/шум от – 20 до +10 дБ с шагом в 2 дБ. В результате экспериментальных исследований установлено, что словесная разборчивость выше 20% наблюдается: для АСР «WhisperX-large-v3» – при отношении сигнал/шум выше минус 8 дБ, для АСР GigaAM-RNNT-v3 – при отношении сигнал/шум выше минус 2 дБ, а при артикуляционных испытаниях – при отношении сигнал/шум выше минус 10 дБ.

В качестве показателя эффективности защиты акустической речевой информации используется словесная разборчивость речи, под которой понимается относительное количество правильно понятых человеком слов из перехваченного разговора [1].

Одним из основных методов оценки разборчивости речи в условиях помех является метод артикуляционных испытаний [2].

Проведение артикуляционных испытаний является довольно трудоемким и дорогим процессом. Например, на прослушивание аудиофайлов для одного вида шума с отношением сигнал/шум от – 20 до +10 дБ с шагом 2 дБ (16 аудиофайлов) одним аудитором уходит от 2,5 до 3 часов и более.

Одним из направлений, существенно снижающих время и стоимость проведения артикуляционных испытаний, является использование технологий искусственного интеллекта.

Цель проводимых исследований – оценить возможность использования технологий искусственного интеллекта для распознавания речи в условиях помех при низких отношениях сигнал/шум.

Проведенный анализ научной литературы показал, что одними из наиболее эффективных систем автоматизированного распознавания русской речи (АСР) являются системы «WhisperX-large-v3» (США) и «GigaAM-RNNT-v3» (Россия) [3 – 5].

Исследования разборчивости речи с использованием АСР проводились в несколько этапов.

На первом этапе проводилась оценка словесной разборчивости речи при высоких отношениях сигнал/шум (исходных тестовых речевых сигналов).

В качестве исходных тестовых речевых сигналов использовались артикуляционные таблицы односложных слов [2]. Запись исходных тестовых речевых сигналов проводилась бригадой из 6-ти дикторов (4 мужчины и 2 женщины), не имеющих дефектов речи.

Для проведения оценки распознавания речи на языке программирования Python было разработано специальное программное обеспечение (СПО) и реализовано в облачной среде выполнения Google colab.

Методика проведения исследований заключалась в следующем:

с использованием СПО аудиофайлы с записями таблиц слов загружались в АСР;

АСР проводила распознавание слов. Результат распознавания записывался в текстовый документ.

Далее при помощи СПО результат приводился к удобной для сравнения форме, фонетически нормализовывался и сравнивался с эталонным текстом, по итогу сравнения рассчитывалось количество правильно распознанных слов по формуле (1):

$$W_{ik} = N_{ik}/N, \quad (1)$$

где W_k – словесная разборчивость аудиофайла с записью слов i -й таблицы, определенная k -м аудитором;

N_{ik} – количество правильно распознанных k -м аудитором слов в аудиофайле с записью слов i -й таблицы (слово считалось правильно понятым АСР, если после нормализации оно совпадало со словом из эталонного текста);

N – общее количество слов в одном аудиофайле ($N= 50$).

Далее результат выражался в процентах.

Результаты оценки словесной разборчивости речи, распознанной АСР «GigaAM-RNNT-v3», приведены в таблице 1.

Таблица 1

Результаты оценки словесной разборчивости речи, распознанной АСР «GigaAM-RNNT-v3»,
при высоких отношениях сигнал/шум

Диктор	Словесная разборчивость речи, %		
	1 таблица	2 таблица	3 таблица
1	62	78	94
2	62	68	78
3	72	74	46
4	58	46	44
5	22	56	24
6	76	54	54
Средняя разборчивость по таблицам	58,67	62,67	56,67
Средняя разборчивость по таблицам и дикторам	59,3 %		

Низкая разборчивость речи (см. таблица 1) очевидно обусловлена тем фактом, что для распознавания использовались таблицы односложных слов, а САР, очевидно, была обучена для распознавания связных текстов, поэтому при распознавании САР объединяла несколько односложных слов в одно.

Далее каждый аудиофайл с записью 50 слов был разбит на 50 аудиофайлов с записью по одному слову. На эту процедуру уходило около 25 минут.

Результаты оценки словесной разборчивости речи таких файлов приведены в таблице 2.

Таблица 2

Результаты оценки разборчивости аудиофайлов с отдельными словами,
распознанной АСР «GigaAM-RNNT-v3», при высоких отношениях сигнал/шум

Диктор	Словесная разборчивость речи, %		
	1 таблица	2 таблица	3 таблица
1	100	100	98
2	94	94	96
3	90	100	94
4	94	84	88
5	94	90	100
6	98	86	96
Средняя разборчивость по таблицам	95	92,3	95,3
Средняя разборчивость по таблицам и дикторам	94,2 %		

Так видно из таблицы 2, словесная разборчивость значительно возросла, но все равно не приблизилась к 100%.

Далее была проведена оценка разборчивости речи аудиофайлов с записями таблиц слов САР «WhisperX-large-v3». Результаты оценки словесной разборчивости речи приведены в таблице 3.

Как видно из таблицы 3, словесная разборчивость речи при высоких отношениях сигнал/шум близка к 100%.

Таблица 3

Результаты оценки словесной разборчивости речи, распознанной АСР «WhisperX-large-v3»,
при высоких отношениях сигнал/шум

Диктор	Словесная разборчивость речи, %				
	1 таблица	2 таблица	3 таблица	4 таблица	5 таблица
1	100	100	100	100	100
2	100	100	100	100	98
3	100	100	100	100	100
4	100	100	100	100	100
5	100	98	100	98	96
6	100	100	98	100	98
Средняя разборчивость по таблицам	100	99,7	99,7	99,7	98,7
Средняя разборчивость по таблицам и дикторам	99,5 %				

На втором этапе проводилась оценка словесной разборчивости зашумленных речевых сигналов.

В качестве шумового сигнала использовался «белый» шум, который генерировался с использованием специального программного обеспечения Adobe Audition 1.5 [6].

При проведении экспериментальных исследований под отношением сигнал/шум понималось среднее отношение речевой сигнал/шум за весь период воспроизведения диктором артикуляционной таблицы. При этом, при измерении уровня сигнала из аудиофайла с записью исходного тестового речевого сигнала удалялись паузы между словами.

Формирование зашумленных тестовых речевых сигналов осуществлялось путем смешения речевых сигналов (исходных тестовых речевых сигналов с паузами) с шумовыми.

Для оценки разборчивости речи были сформированы аудиофайлы с отношениями сигнал/шум от – 20 до +10 дБ с шагом в 2 дБ.

Учитывая значительное время формирования аудиофайлов с записью отдельных слов с требуемым отношением сигнал/шум для распознавания АСР «GigaAM-RNNT-v3», для оценки разборчивости речи использовались аудиофайлы с записями слов из одной таблицы. Результаты распознавания зашумленных тестовых речевых сигналов АСР «GigaAM-RNNT-v3» приведены в таблице 4.

Таблица 4

Результаты оценки разборчивости зашумленной речи для белого шума
АСР «GigaAM-RNNT-v3» (диктор 1, таблица 1)

Отношение сигнал/шум, дБ	Словесная разборчивость речи, %	Отношение сигнал/шум, дБ	Словесная разборчивость речи, %
–20	0	–4	18
–18	0	–2	28
–16	0	0	36
–14	0	2	46
–12	0	4	60
–10	2	6	68
–8	6	8	78
–6	8	10	82

Результаты распознавания зашумленных тестовых речевых сигналов АСР «WhisperX_large-v3» приведены в таблице 5.

Таблица 5

Результаты оценки разборчивости зашумленной речи для белого шума
АСР «WhisperX_large-v3» (таблица 1)

Отношение сигнал/шум, дБ	Словесная разборчивость речи, %						
	Диктор 1	Диктор 2	Диктор 3	Диктор 4	Диктор 5	Диктор 6	$\bar{W}_{cp}$
–20	0	0	0	0	0	0	0
–18	0	0	0	0	0	0	0
–16	0	0	0	0	0	0	0
–14	0	0	0	0	0	0	0
–12	0	0	4	0	4	4	2
–10	0	16	16	26	4	12	12,3
–8	24	20	32	36	6	28	24,3
–6	30	30	48	46	12	56	37
–4	52	52	62	58	18	56	49,7
–2	54	60	68	60	28	64	55,8
0	60	76	74	66	38	80	65,8
2	68	76	80	70	40	80	69
4	72	82	90	–	48	88	76
6	88	90	90	78	56	90	82
8	94	90	94	82	70	94	87,3
10	96	90	94	88	76	96	90

Для сравнения в таблице 6 приведены результаты оценки словесной разборчивости зашумленной речи для белого шума, проведенной с использованием АСР, и полученные методом артикуляционных испытаний с привлечением 8 аудиторов [7].

Таблица 6

Результаты оценки словесной разборчивости зашумленной речи для белого шума, проведенной с использованием АСР, и проведенной методом артикуляционных испытаний с привлечением 8 аудиторов
(для средних значений)

Отношение сигнал/шум, дБ	Словесная разборчивость речи, %		
	«GigaAM-RNNT-v3»	«WhisperX-large-v3»	Артикуляционные испытания (8 аудиторов)
-20	0	0	1
-18	0	0	2
-16	0	0	6
-14	0	0	12
-12	0	2	19
-10	2	12,3	26
-8	6	24,3	35
-6	8	37	40
-4	18	49,7	48
-2	28	55,8	55
0	36	65,8	62
2	46	69	69
4	60	76	74
6	68	82	80
8	78	87,3	84
10	82	90	86

Анализ результатов экспериментальных исследований показал, что:

- при высоких отношениях сигнал/шум (при отсутствии помех) средняя разборчивость коротких слов по ГОСТ 16600 – 72 составляет: для АСР «WhisperX-large-v3» – 99,5%, для АСР «GigaAM-RNNT-v3» – 59,3 % (94,2% – при использовании записей слов по отдельности);
- при отношениях сигнал/шум выше или равно – 6 дБ разборчивость зашумленных речевых сигналов, полученная АСР «WhisperX-large-v3», составляет более 30% и сопоставима с разборчивостью, полученной по результатам артикуляционных испытаний;
- разборчивость зашумленных речевых сигналов, полученная АСР «WhisperX-large-v3» при отношении сигнал/шум от – 12 дБ до – 6 дБ не включительно, значительно ниже разборчивости, полученной по результатам артикуляционных испытаний, а при отношении сигнал/шум ниже – 12 дБ близка к нулю;
- при отношениях сигнал/шум выше – 12 дБ разборчивость зашумленных речевых сигналов, полученная АСР «GigaAM-RNNT-v3», значительно ниже разборчивости, полученной АСР «WhisperX-large-v3».

Следовательно, при отношениях сигнал/шум выше или равно – 6 дБ артикуляционные испытания могут проводиться с использованием АСР «WhisperX-large-v3».

Литература

1. Хорев А.А. Оценка возможностей средств акустической (речевой) разведки//Специальная техника. – М.: 2009. – № 4 – С. 49-63.
2. ГОСТ 16600-72. Передача речи по трактам связи радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений. – Введ. 1972-09-27. М.: Государственный комитет стандартов совета министров СССР, 1972. – 93 с.
3. Radford A., Kim J.W., Xu T., Brockman G., McLeavey C., Sutskever I. Robust Speech Recognition via Large-Scale Weak Supervision // Proceedings of the 40th International Conference on Machine Learning (ICML 2023). – Honolulu, Hawaii, USA, 2023. – С. 28492-28518.
4. Bain M., Huh J., Han T., Zisserman A. WhisperX: Time-Accurate Speech Transcription of Long-Form Audio// Препринт. – Oxford, 2024. – С. 1-6.

5. Kutsakov A., Maximenko A., Gospodinov G., Bogomolov P., Minkin F. GigaAM: Efficient Self-Supervised Learner for Speech Recognition // Труды конференции Interspeech 2025. – Rotterdam, The Netherlands, 2025. – С. 1-5.
6. Adobe AUDITION 1.5: Руководство пользователя. [Электронный ресурс]. – Режим доступа: <https://www.manualslib.com/manual/1995/Adobe-Audition-1-5.html>.
7. Хорев А.А. Экспериментальные исследования разборчивости речи в условиях помех// Всероссийская конференция «Радиоэлектронные устройства и системы для инфотелекоммуникационных технологий – РЭУС-2026». Доклады. – М.: РНТОРЭС имени А.С. Попова. 2026. – С. ISBN 978-5-905278-62-4

RESEARCH OF SPEECH DIARRY IN INTERFERENCE CONDITIONS USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Prof. Horev A.A., stud. Molozhavgtey E.O.

National Research University of Electronic Technology

The article presents the results of experimental studies of the intelligibility of speech signals using artificial intelligence technologies. The "WhisperX-large-v3" and GigaAM-RNNT-v3 systems were used as automated recognition systems (ARS), and articulation tables of monosyllabic words were used as the initial test speech signals. According to the results of the experimental studies, the verbal intelligibility of the original test speech signals was 99.5% for the "WhisperX-large-v3" ASR and 94.2% for the GigaAM-RNNT-v3 ASR. The noisy speech signals were generated by mixing the original test speech signals with white noise at signal-to-noise ratios ranging from -20 to +10 dB in 2 dB increments. As a result of experimental studies, it was found that verbal intelligibility above 20% is observed: for the "WhisperX-large-v3" ASR, at a signal-to-noise ratio above minus 8 dB; for the GigaAM-RNNT-v3 ASR, at a signal-to-noise ratio above minus 2 dB, and for articulation tests, for signal-to-noise ratios above minus 10 dB.



ИСПОЛЬЗОВАНИЕ ЗОНАЛЬНОЙ МОДЕЛИ ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ ДЛЯ ФОРМУЛИРОВКИ ТРЕБОВАНИЙ ПОЛИТИКИ БЕЗОПАСНОСТИ КИИ ПО КОНТРОЛЮ ВХОДЯЩЕГО И ИСХОДЯЩЕГО ТРАФИКА.

доц., к.т.н., Петухов А.Н.¹, к.т.н. Пилюгин П.Л.^{1,2}, студ. Назаров М.Э.²

¹Национальный исследовательский университет «МИЭТ»

²Московский государственный университет им. М.В.Ломоносова «МГУ»

Обсуждаются аспекты обеспечения информационной безопасности при взаимодействии с глобальной вычислительной сетью интернет. Отмечается важность достижения целей обеспечения целостности и доступности для КИИ. Анализируются слабости существующего протокола маршрутизации BGP. Предлагается дополнять политику безопасности функцией интеллектуальным фильтром, для межсетевого экрана КИИ при этом в рамках данной работы не решается задача классической маршрутизации (поиска «оптимального» пути доставки пакета) в отдельных случаях этот фильтр может быть использован. В основе политики лежит зональная модель контроля потоков, а для формулировки критерия безопасности потока использована модель контроля целостности Биба? в качестве элементов которой выступают зоны: отдельные AS или группы AS. В результате в зависимости от политики и значимости конкретного объекта КИИ, трафик, прибывший или отправляемый по опасному или недоверенному маршруту может блокироваться. Главная цель такой политики — аппаратно или программно не допустить прямого взаимодействия «грязных» данных с «чистыми» критичными ресурсами внутренней сети.

При взаимодействии любых КИИ с глобальной вычислительной сетью интернет или использования ее для построения VPN каналов должны решаться вопросы изоляции передаваемого трафика и (или) его фильтрации. В первом случае используются криптографические средства, а во втором межсетевые экраны соответствующей категории [1]. И в том и в другом случае должны быть определены IP адреса взаимодействующих пиров, используемые ими порты. Для установления VPN соединения требуется синхронизация характеристик безопасности обеих сторон, а для более детальной фильтрации трафика анализируются также флаги заголовков пакетов и дейтаграмм, в некоторых случаях и содержимое передаваемых данных DPI (Deep Packet Inspection) [2]. При этом маршрут доставки пакетов, который может содержать до 256 промежуточных узлов глобальной сети, не учитывается и может стать причиной нежелательных инцидентов.

Проблемы безопасности маршрутов в глобальной сети интернет связаны с протоколом BGP4 (Border Gateway Protocol), актуальная версия которого используется более 20 лет [3]. Основная функция протокола BGP заключается в обмене информацией (анонсами) между серверами, поддерживающими протокол BGP, о доступности автономной сети с другими. Информация о доступности сети включает сведения о списке автономных систем (AS), через которые проходит информация о доступности автономных систем. Эти данные достаточны для динамического построения маршрутов по передаче трафика из одной автономной системы другую, и организации связности всей сети.

Сегодня атаки на интернет как глобальную сеть, связаны, в том числе, с исторически наследуемыми уязвимостями протокола динамической маршрутизации BGP [4]. Все атаки на BGP маршрутизацию условно можно разделить на 2 группы. Первая группа атак направлена на инфраструктуру маршрутизации: спуфинг и имперсонация серверов BGP и каналов связи между ними, что позволяет внедрять ложную маршрутную информацию. Для защиты от таких атак предложены механизмы, дополняющие протокол BGP [5]. Вторая проблема безопасности связана с распространением ложной или просто ошибочной информации, что собственно и может привести к нежелательным инцидентам [6]. Источником такой информации могут являться как объекты атакованной BGP инфраструктуры, так ошибочные или злонамеренные действия легитимных администраторов промежуточных серверов BGP. С точки зрения последствий возможных атак на BGP выделяют:

- утечки маршрутов BGP (BGP route leak);
- перехват или «угон» BGP (BGP route hijacking).

BGP route leak — технически представляет собой ситуацию, когда префикс BGP сервера, описывающий доступные маршруты, полученный AS от одного вышестоящего провайдера или пира некорректно анонсируется другому вышестоящему провайдеру или пиру. То есть AS объявляет, что через нее доступны другие автономные системы, связи с которыми у нее на самом деле нет. Это приводит к перестроению маршрутов во все сети и в результате информация утекает в никуда или в лучшем случае отправляется не оптимальным, удлинненным маршрутом.

BGP route hijacking — технически это такая настройка протокола BGP, при которой автономная система (AS) незаконно объявляет через BGP чужие IP-префиксы, перенаправляя трафик через свои сети [7]. Если эти действия происходят в результате сознательной атаки, то злоумышленник может: анализировать

или модифицировать трафик, вызывать DoS (отбрасывание пакетов) или перенаправлять трафик по своему выбору (например, в фишинговые сети).

Несмотря на незащищенность протокола BGP считается BGP Route leaking и hijacking происходят из-за ошибок в конфигурировании протокола BGP, и таких «утечек» и «перехватов» ежедневно происходит десятки и сотни. Но и «утечка» и «перехват» могут быть также и результатом злоумышленных действий. В любом случае они вызывают инциденты: иногда это задержки или потеря данных, а порой атаки DOS или MITM. Отметим, что для КИИ часто не важна причина такого инцидента вся проблема в нарушении функционирования КИИ и в последствиях для критически-важных объектов. Так же нужно отметить, что результаты таких «утечек» и «перехватов» в виде новых маршрутов доступны для анализа. Кроме того следует иметь ввиду, что средства обеспечения безопасности КИИ должны учитывать возможность появления потенциально опасных маршрутов и не в результате «утечек» и «перехватов».

Целями обеспечения информационной безопасности КИИ как и в общем случае являются конфиденциальности, целостность и доступность. Однако, с учетом специфики информации в таких системах можно переопределить важность рассматриваемых целей. В первую очередь для большинства КИИ (АСУ ТП, Транспорт, Связь, Энергетика и т.д.) наиболее актуально обеспечение целостности и доступности информации. При этом если для обеспечения конфиденциальности передаваемой информации достаточно использовать сертифицированные криптографические средства, изолирующие VPN для КИИ от глобальной сети, то для обеспечения целостности и доступности передаваемой информации необходимо учитывать характеристики маршрутов, по которым эта информация передается. Действительно, даже построение VPN канала через маршрут, который может вести в никуда: «захват трафика» или «утечка маршрута» может нарушить работоспособность КИИ. В то же время использование «перенаправления трафика» позволяет проводить его анализ в произвольной сети, том числе и обладающей вычислительными ресурсами для анализа зашифрованной информации. А в случае отрытой информации или компрометации шифрованного канала навязывать недостоверную или сфабрикованную информацию.

Для противодействия подобным атакам политика безопасности КИИ может предусматривать правила разрешения и запрещения входящего или исходящего трафика, если он передается через «опасный» или «ненадежный» маршрут. Формальное описание политики безопасности предполагает описание правил, по которым разрешается или запрещается информационный поток. Наиболее наглядное представление о механизме защиты, реализующем такую политику на сетевом уровне, дает межсетевой экран. Применительно к рассматриваемому случаю политика должна использовать характеристики маршрута, по которому пересылается информация. Формально такие характеристики можно представить в качестве некоего интегрального показателя «доверия» к маршруту, а саму политику как проверку значения «допустимости» этого показателя. В основу такой политики безопасности можно положить мандатную модель целостности Биба.

Модель контроля целостности Биба, предложенная Кеннет Дж. Биба в 1977 году в рамках исследований для MITRE Corporation [8], была разработана как концептуальная альтернатива доминировавшим на тот момент моделям информационной безопасности. В отличие от модели Белла-ЛаПадулы, ориентированной на обеспечение конфиденциальности и предотвращение утечек, модель Биба сосредоточена на задаче защиты целостности данных — то есть предотвращении их несанкционированного или искажающего изменения. Ключевая идея модели заключается в ограничении влияния менее надёжных субъектов на критически важные данные, а также в предотвращении ситуаций, при которых доверенные процессы могут быть скомпрометированы за счёт использования недостоверной информации. Для этого каждому субъекту (например, пользователю или процессу) и объекту (файлу, потоку данных или маршруту) назначается уровень целостности, формирующий иерархию доверия [9].

В контексте современных сетевых технологий и защиты критической информационной инфраструктуры логика модели Биба хорошо соотносится с архитектурой зональной политики обеспечения безопасности. Зональная модель — предполагает подход к организации защиты информации, при котором ресурсы и системы разделяются на зоны (сегменты) в зависимости от уровня их требований к безопасности (конфиденциальности, целостности и доступности). Каждая зона имеет свои правила доступа, политики безопасности и механизмы защиты. Под зональной политикой безопасности в данном контексте в первую очередь понимаются правила взаимодействия между зонами. То есть возможность организации информационных потоков между объектами различных зон. Существуют одноуровневые отношения доверия (односторонние и двусторонние) и иерархические отношения, требованиями безопасности.

В соответствии с правилами мандатной политики Биба допускаются информационные потоки «сверху вниз» по принятой иерархии классов или на одном уровне (правила No Write Up» и «No Read

Down»). В качестве взаимодействующих субъектов модели предлагается рассматривать зоны, состоящие из отдельных, AS или связанных групп AS с общей политикой безопасности, а протокол BGP является их транспортной основой.

Для реализации указанной политики необходимо «раскрасить» входящий в КИИ трафик интернет, то есть в соответствии с правилами мандатной модели расставить метки доверия маршрутам и сравнить его с пороговым значением политики. В качестве такой метки маршрута может выступать интегральный показатель совокупности меток AS, входящих в этот маршрут. Причем в качестве метки AS может выступать качественное значение: класс или категория, установленным отношением порядка на множестве классов или количественное значение, которое будем называть индексом доверия AS. Например, если для качественных меток AS можно определять метку маршрута как наибольшую или наименьшую метку AS (или как наименьшую верхнюю или наибольшую нижнюю границу для иерархии, образующей алгебраическую решетку) [10]. Для количественных значений меток AS могут использоваться как максимальное и минимальное значение меток, так и различные методы усреднения.

В качестве методов получения значений меток AS наиболее очевидным является метод экспертных оценок. Однако существующее количество AS позволяет использовать его в ограниченном объеме, например, только для AS наиболее часто используемых в маршрутах для КИИ. Однако, экспертные оценки позволяют строить как качественные так и количественные метки. Все непомеченные маршруты будут рассматриваться как неподтвержденные. Следовательно, например, при фильтрации в КИИ маршрутов BGP любой внешний трафик или только неподтвержденные маршруты могут рассматриваться как объекты с низким уровнем целостности. В соответствии с принципом «No Write Up» такой трафик не должен иметь прямого доступа к внутренним сегментам сети.

В качестве вариантов в качестве методов построения меток доверия AS можно использовать методы больших данных для кластеризации и классификации множества существующих AS, а для частично полученных значений меток вычисление значения для смежных меток по критерию близости на графе связности.

Отметим, что в рамках данной работы не решается задача классической маршрутизации (поиска «оптимального» пути доставки пакета). Это связано с тем, что политики отдельных зон могут не только не совпадать, но и преследовать различные цели, оставаясь, однако в принятых правилах взаимодействия AS.

Важно, что предлагаемый подход выполняет функцию интеллектуального фильтра, прежде всего, для межсетевого экрана КИИ. В зависимости от политики и значимости конкретного объекта КИИ, трафик, прибывший или отправляемый по опасному или недоверенному маршруту может блокироваться. Формальным критерием для допуска или недопуска трафика является превышение установленного «порогового» значения, когда трафик можно считать «допустимым». Главная цель такой политики — аппаратно или программно не допустить прямого взаимодействия «грязных» данных с «чистыми» критичными ресурсами внутренней сети. Однако прибывший трафик может не обязательно подвергаться немедленному уничтожению. Опираясь на принципы мандатного контроля, такой трафик должен помеченный межсетевым экраном как «грязный» (обладающий низким уровнем целостности) для сохранения функциональности системы может пройти «очистку», используя механизмы контролируемого повышения доверия. Его реализуют, например, системы глубокого анализа пакетов (DPI) и системы предотвращения вторжений (IPS), которые выполняют детальную проверку содержимого трафика. В случае успешной валидации данные могут получить более высокий уровень целостности и быть допущены к взаимодействию с защищенной инфраструктурой [11].

Литература

1. Юдин А.П., Резниченко С.А. Аудит информационной безопасности КИИ: особенности и требования. Флагман науки. 2024. № 3 (14). С. 364-368.
2. Гольдштейн Б.С., Фицов В.В. Глубокая инспекция пакетов DPI: проблемы и подходы. Вестник связи. 2018. № 9. С. 5 - 10.
3. RFC 4271 BGP-4 January 2006. [ietf.org/rfc/rfc4271.txt](https://www.rfc-editor.org/rfc/rfc4271.txt)
4. RFC 4272 BGP Security Vulnerabilities Analysis [Электронный ресурс]. URL: <https://datatracker.ietf.org/doc/html/rfc4272> (дата обращения: 18.05.2025).
5. RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option [Электронный ресурс]. URL: <https://www.rfc-editor.org/rfc/rfc2385.html> (дата обращения: 18.05.2025).

6. RFC 7908 Problem Definition and Classification of BGP Route Leaks [Электронный ресурс]. URL: <https://www.rfc-editor.org/rfc/rfc7908.html> (дата обращения: 18.05.2025).
7. Робачевский А. Безопасный пиринг // Интернет изнутри. 2015. №7. С. 38–45.
8. Биба К. Дж. Вопросы целостности для защищенных компьютерных систем. — MTR-3153. — The Mitre Corporation, июнь 1975.
9. Bishop, M. Computer Security: Art and Science. — 2nd ed. — Addison-Wesley Professional, 2018. — 1392 p.
10. Гайдамакин, Н.А. Учебно-методический комплекс дисциплины "Теоретические основы компьютерной безопасности" Урал. гос. ун-т им. А. М. Горького 2008.
<https://elar.urfu.ru/handle/10995/1778?ysclid=mohj72ectv127877542>
11. Pfleeger, C. P., Pfleeger, S. L., Margulies, J. Security in Computing. — 5th ed. — Prentice Hall, 2015.

USING A ZONAL MODEL OF THE GLOBAL INTERNET TO FORMULATE THE REQUIRED SECURITY POLICIES FOR CII TRAFFIC CONTROL POLICY

PhD Petukhov A.N.¹, PhD Pilyugin P.L.^{1,2}, student. Nazarov M.E.²

¹National Research University "MIET"

²Lomonosov Moscow State University "MSU"

The aspects of ensuring information security when interacting with the global computer network Internet are discussed. The importance of achieving the goals of ensuring the integrity and accessibility of CII is noted. The weaknesses of the existing BGP routing protocol are analyzed. It is proposed to supplement the security policy function with an intelligent filter, while for the CII firewall, the task of classical routing (finding the "optimal" packet delivery path) is not solved in this work. In some cases, this filter can be used. The policy is based on the zonal flow control model, and the Biba integrity control model was used to formulate the flow safety criterion, the elements of which are zones: individual AS or groups of AS. As a result, depending on the policy and significance of a particular CII facility, traffic arriving or departing via a dangerous or untrusted route may be blocked. The main goal of such a policy is to prevent hardware or software from direct interaction of "dirty" data with "clean" critical resources of the internal network.



РАЗРАБОТКА СРЕДСТВА МОНИТОРИНГА И ОБНАРУЖЕНИЯ АТАК НА БЕСПРОВОДНЫЕ СЕТИ Wi-Fi

студ. Николаев Р.С.

Национальный исследовательский университет «МИЭТ»

В работе разработан программный прототип средства мониторинга на базе одноплатного компьютера Raspberry Pi 4, реализующий сигнатурный метод обнаружения атак. Определены сигнатуры для выявления атак деаутентификации, подмены точки доступа, перебора WPS PIN и атаки KRACK. Проведённые экспериментальные исследования подтвердили способность разработанного средства обнаруживать указанные типы атак в соответствии с заданными пороговыми значениями. Полученные результаты демонстрируют возможность применения разработанного средства в учебных целях для изучения атак на беспроводные сети, а также для повышения уровня защищённости беспроводных сегментов сети.

Введение

В условиях цифровизации и повсеместного внедрения беспроводных технологий сети Wi-Fi стали неотъемлемой частью не только корпоративной инфраструктуры, но и повседневной жизни. Данное изобретение позволяет снизить затраты на развёртывание сетевой инфраструктуры, однако за этим преимуществом стоит существенная проблема – обеспечение защиты информации. Радиочастотный канал по своей природе является открытой средой передачи, что делает беспроводные сети уязвимыми для широкого спектра атак со стороны неавторизованных устройств.

Современные беспроводные сети подвержены многочисленным атакам, к которым относятся: деаутентификация клиентов, подмена точек доступа, перебор WPS PIN, атака KRACK, а также несанкционированное подключение к сети. Усложнение архитектуры Wi-Fi, использование схем с гостевыми и корпоративными сегментами, рост числа устройств интернета вещей значительно увеличивают поверхность атаки и усложняют контроль безопасности.

Множество точек доступа продолжают работать на протоколе WPA2, что связано с отсутствием поддержки WPA3 на устаревшем оборудовании. Несмотря на улучшения безопасности в WPA3, использование встроенных технологий не обеспечивает достаточного уровня защищённости в условиях целенаправленных атак, которые могут остаться незамеченными.

Существующие маршрутизаторы ориентированы преимущественно на предотвращение несанкционированного доступа в сеть, но не обеспечивают мониторинг радиоэфира. Отсутствие централизованного мониторинга затрудняет выявление атак и последующий анализ инцидентов.

В связи с этим разработка средства мониторинга и обнаружения атак на беспроводные сети Wi-Fi является актуальной задачей. В рамках данной работы ставится задача создания такого средства, обеспечивающего: выявление атак деаутентификации, подмены точки доступа, перебора WPS PIN и KRACK; регистрацию событий в журнале; работу в режиме, близком к реальному времени.

Целью работы является разработка средства мониторинга и обнаружения атак на беспроводные сети Wi-Fi, обеспечивающей выявление вредоносной активности в сети и регистрацию атак.

Основная часть

Беспроводные сети Wi-Fi строятся на основе передачи данных с помощью электромагнитных волн. В отличие от проводных сетей, где среда передачи ограничена кабелем, в Wi-Fi средой является радиоэфир. Точка доступа выполняет роль моста между беспроводной и проводной сетью, а также управляет подключениями в своей локальной сети. Клиентские устройства инициируют процесс подключения и передачу данных. Устройства работают в полудуплексном режиме, а для решения коллизий используется множественный доступ с контролем несущей и предотвращением коллизий.

Эволюция стандартов IEEE 802.11 прошла путь от 802.11a/b до 802.11ax. Развитие шло по пути увеличения скорости: от 11 Мбит/с до нескольких гигабит в секунду, внедрения технологий MIMO, MU-MIMO, OFDMA и работы в нескольких диапазонах.

Механизмы безопасности также эволюционировали. Протокол WEP использовал статический ключ шифрования и был признан устаревшим к 2004 году. Ему на смену пришёл WPA с протоколом TKIP, а затем WPA2 с алгоритмом AES и протоколом CCMP. Современный WPA3 внедрил протокол SAE и устойчивость к атакам перебора паролей, однако сохраняет совместимость с WPA2, что создает дополнительные уязвимости.

В работе проведён анализ актуальных атак на беспроводные сети.

Атака деаутентификации заключается в массовой рассылке поддельных кадров деаутентификации, которые не шифруются и не требуют подтверждения подлинности даже в сетях WPA2/WPA3.

Злоумышленник отправляет такие кадры от имени точки доступа, принудительно отключая клиентские устройства. Это позволяет реализовывать атаки типа «отказ в обслуживании» и подготавливать условия для других атак.

Взлом паролей WPA/WPA2 основан на перехвате четырёхэтапного рукопожатия при подключении клиента. Злоумышленник пассивно прослушивает эфир, сохраняет кадры EAPOL, содержащие nonce и MIC, после чего выполняет офлайн-перебор пароля с использованием специализированных средств. Сложность атаки определяется исключительно стойкостью пароля.

Взлом WPS использует уязвимость протокола Wi-Fi Protected Setup, где 8-значный PIN-код проверяется по частям: сначала 4 цифры, затем 3 значащие цифры. Общее количество комбинаций составляет не 100 миллионов, а всего 11 тысяч, что делает перебор тривиальным за несколько часов.

Атака подмены точки доступа заключается в создании фальшивой точки доступа с доверенным SSID и более мощным сигналом. В сочетании с атакой деаутентификации клиенты переподключаются к фальшивой точке, после чего злоумышленник может перехватывать и анализировать трафик, а также реализовывать фишинговые атаки.

Атака KRACK использует уязвимость в четырёхэтапном рукопожатии WPA2. Злоумышленник многократно повторно отправляет третье сообщение рукопожатия, вызывая переустановку уже использованного сеансового ключа с обнулением счётчика пакетов, что позволяет расшифровывать трафик.

Для построения системы мониторинга проведён анализ методов обнаружения атак.

Методы обнаружения аномалий основаны на выявлении отклонений от модели нормального поведения. Они способны обнаруживать неизвестные атаки, но характеризуются высоким уровнем ложных срабатываний, требуют накопления статистики и значительных вычислительных ресурсов.

Сигнатурный метод основан на поиске в трафике заранее известных признаков атак. Он обеспечивает высокую достоверность для известных угроз, минимальный уровень ложных срабатываний, высокую скорость обработки и низкие требования к ресурсам. Основным недостатком является невозможность обнаружения новых атак.

Для Wi-Fi сетей характерно, что большинство атак реализуется по давно известным сценариям, а новые векторы атак появляются редко. Поэтому сигнатурный метод выбран в качестве основного подхода для реализации системы мониторинга.

На основе проведённого анализа разработана архитектура программного средства (рисунок 1).

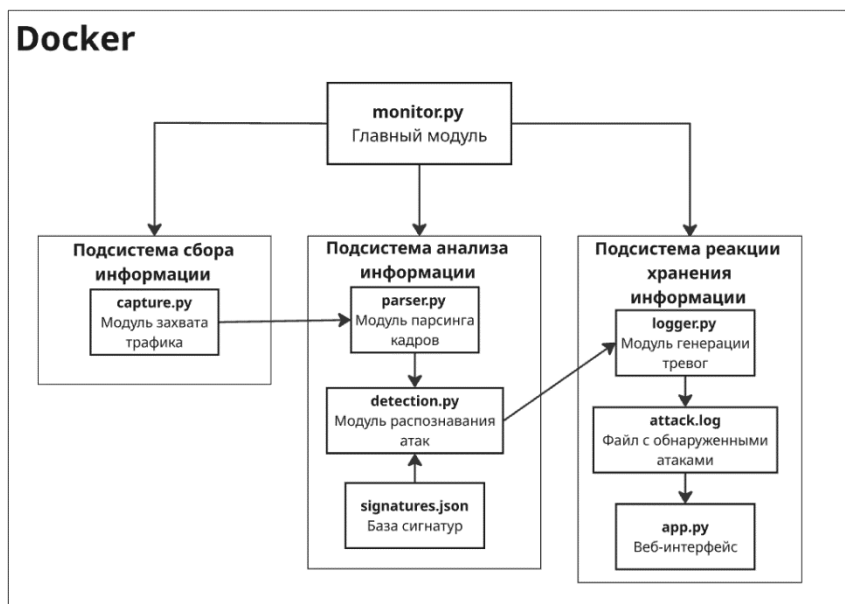


Рисунок 8 - Архитектура программного средства мониторинга

Разработанное средство включает следующие модули:

- модуль захвата трафика – переводит Wi-Fi адаптер в режим мониторинга, выполняет перехват кадров 802.11 и помещает их в очередь;
- модуль парсинга кадров – извлекает из сырых кадров значимые поля: тип кадра, MAC-адреса, SSID, информацию EAPOL и WPS;
- модуль обнаружения атак – реализует сигнатурный метод, анализирует статистику кадров и выявляет признаки атак;

- модуль логирования – сохраняет обнаруженные атаки в журнал в формате JSON с ротацией при достижении 100 МБ;
- веб-интерфейс – предоставляет пользователю возможность просмотра статистики и журнала атак через браузер;
- главный модуль – координирует работу всех компонентов.

Для каждого типа атаки определена сигнатура с параметрами порога срабатывания и временного окна (таблица 1).

Таблица 1

Сигнатуры обнаруживаемых атак

Тип атаки	Идентификатор	Порог	Временное окно
Деаутентификация	WIFI_DEAUTH_FLOOD	10 кадров	5 секунд
Перебор WPS PIN	WIFI_WPS_BRUTE	5 сообщений	30 секунд
KRACK	WIFI_KRACK_ATTACK	2 повторных msg3	10 секунд
Evil Twin	WIFI_EVIL_TWIN	Накопление beacon-сообщений	30 секунд

В качестве аппаратной платформы выбран одноплатный компьютер Raspberry Pi 4 Model B. Проведён сравнительный анализ, показавший преимущества данной платформы: оптимальное соотношение производительности и энергопотребления, компактность, низкая стоимость, полноценная поддержка Linux и режима мониторинга.

Разработанное программное средство реализовано на языке Python с использованием библиотек Scapy и Flask. Для упрощения развёртывания средство упаковано в Docker-контейнер с необходимыми привилегиями для доступа к беспроводному интерфейсу.

Для проверки работоспособности разработанного средства проведено функциональное тестирование на лабораторном стенде (рисунок 2).

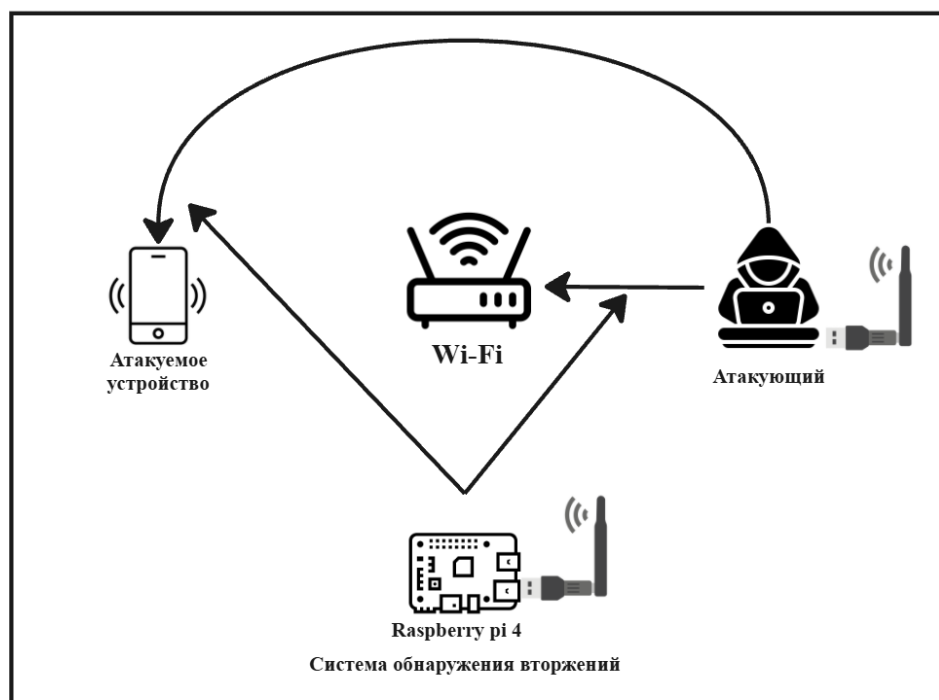


Рисунок 9 - Схема лабораторного стенда

В составе стенда использовались: Raspberry Pi 4 с разработанным средством мониторинга, Wi-Fi адаптер TP-LINK Archer T3U Plus, ноутбук с Kali Linux для генерации атак, Wi-Fi роутер Keenetic Lite KN-1311 и мобильный телефон.

Тестирование атаки деаутентификации проводилось с использованием инструмента aireplay-ng. При отправке 10 и более кадров деаутентификации в течение 5 секунд средство мониторинга успешно зафиксировало атаку, сформировало оповещение с указанием MAC-адресов источника, цели и количества пакетов.

Тестирование атаки перебора WPS PIN проводилось с использованием инструмента airgeddon. При превышении порога в 5 WPS-сообщений за 30 секунд система сформировала оповещение с фиксацией атакующего устройства и целевой точки доступа.

Тестирование атаки Evil Twin проводилось путём создания фальшивой точки доступа с SSID доверенной сети. Средство мониторинга обнаружило появление beacon-кадров с доверенным SSID, но неизвестным BSSID, и после 30 секунд накопления сформировало оповещение с перечислением подозрительных MAC-адресов.

Тестирование атаки KRACK проводилось с использованием тестового скрипта, многократно повторно отправлявшего перехваченный кадр EAPOL Message 3. При обнаружении 2 и более повторных передач с одинаковым поппе за 10 секунд система успешно идентифицировала атаку.

Результаты тестирования подтвердили способность разработанного средства обнаруживать все четыре типа атак в соответствии с заданными сигнатурами. Во всех случаях система корректно формировала оповещения, сохраняла информацию в журнал событий и отображала в веб-интерфейсе.

Анализ результатов

В результате выполнения работы проведён анализ архитектуры и механизмов безопасности Wi-Fi, актуальных атак. Обоснован выбор сигнатурного метода обнаружения. Спроектирована и реализована модульная архитектура программного средства на базе Raspberry Pi 4. Определены сигнатуры для обнаружения четырёх типов атак с определенными пороговыми значениями.

Функциональное тестирование подтвердило работоспособность средства: система корректно формирует оповещения, фиксирует MAC-адреса участников и сохраняет события в журнал.

К основным преимуществам средства относятся: низкий уровень ложных срабатываний, модульность архитектуры, работа в реальном времени, компактность и низкая стоимость платформы, контейнеризация с использованием Docker.

Полученные результаты демонстрируют возможность применения разработанного средства в учебных и практических целях для повышения защищённости беспроводных сетей.

Литература

1. Остапенко А.Г., Иванкин М.П., Савенков Г.А. Обнаружение и нейтрализация вторжений в распределенных информационных системах. - 1-ое изд. - Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2013. - 87 с.
2. Васильев В.И., Шарабыров И.В. Обнаружение атак в локальных беспроводных сетях на основе интеллектуального анализа данных // Известия ЮФУ. Технические науки. - 2014. - №151. - С. 57-67.

DEVELOPMENT OF A TOOL FOR MONITORING AND DETECTING ATTACKS ON WIRELESS Wi-Fi NETWORKS

Stud. Nikolaev R.S

National Research University of Electronic Technology

This paper developed a software prototype for a monitoring tool based on a Raspberry Pi 4 single-board computer, implementing a signature-based attack detection method. Signatures were defined to detect deauthentication attacks, access point spoofing, WPS PIN brute-force attacks, and KRACK attacks. Experimental studies confirmed the developed tool's ability to detect these types of attacks according to specified thresholds. The obtained results demonstrate the potential of the developed tool for educational purposes, studying attacks on wireless networks, and improving the security of wireless network segments.



ПРИМЕНЕНИЕ КВАЛИМЕТРИЧЕСКОЙ ОЦЕНКИ ПРИ ПРОВЕДЕНИИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

асп. Нилов Н.А., проф. Душкин А.В.

Национальный исследовательский университет «МИЭТ»

В статье поднимается вопрос проблемы несоответствия между растущим объемом нормативных требований к защите критической информационной инфраструктуры (КИИ) Российской Федерации и отсутствием объективных методик количественной оценки их выполнения. Проведен сравнительный анализ отечественных нормативных актов и международных стандартов, в ходе которого установлено принципиальное методологическое расхождение на метрическом уровне: российская регуляторика оперирует качественными, бинарными оценками, тогда как мировая практика переходит к количественному измерению эффективности и зрелости процессов. Предложена двухуровневая квалиметрическая модель оценки, синтезирующая обязательные требования регулятора с принципами СММИ. Модель включает: расчет базового показателя выполнения «гигиенического минимума» и интегральную оценку зрелости по пяти доменам (идентификация, защита, обнаружение, реагирование, восстановление) на основе порядковой шкалы и весовых коэффициентов. Внедрение предлагаемого подхода позволяет преодолеть существующее противоречие, объективизировать результаты аудита и создать стимулы для непрерывного совершенствования систем защиты КИИ в условиях эскалации киберугроз.

Современный этап развития информационного общества характеризуется эскалацией угроз в киберпространстве, что особенно остро проявляется в отношении субъектов критической информационной инфраструктуры (КИИ) Российской Федерации. В условиях геополитической напряженности целенаправленные компьютерные атаки на КИИ приобрели характер инструмента гибридного воздействия, ставя под прямую угрозу национальный суверенитет государства. Данный тезис неоднократно подчеркивался высшим руководством страны и послужил катализатором для системного реформирования нормативно-правовой базы.

С принятием Федерального закона от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – 187-ФЗ) начался этап комплексного государственного регулирования, результатом которого к 2025 году стало многократное увеличение массива подзаконных актов и ведомственных приказов, детализирующих требования к системам защиты КИИ. Практика контрольно-надзорной деятельности ФСТЭК России демонстрирует тревожную тенденцию: количественное расширение регуляторных требований не конвертируется в качественный рост защищенности КИИ. Согласно опубликованным данным ведомства за 2025 год, по итогам проверок более 700 значимых объектов было выявлено свыше 1200 нарушений требований безопасности, составлено 603 протокола об административных правонарушениях. Наиболее показательным является тот факт, что лишь 36% проверенных организаций сумели подтвердить достижение необходимого уровня защищенности [1].

Сложившаяся ситуация обнажает ключевое методологическое противоречие: при наличии детализированных требований в Приказах ФСТЭК России №235, №239 и др., в отечественной регуляторике отсутствует утвержденная методика количественной (квалиметрической) оценки степени их выполнения. Исследования таких авторов, как Вульфин А.М., Душкин А.В., Кочедыков С.С., Лившиц И.И., Макаренко С.И. подтверждают выявленное противоречие. Работы указанных авторов заложили фундамент в области моделирования угроз и анализа рисков КИИ, однако они либо частично утратили актуальность в свете последних изменений нормативной базы, либо сфокусированы на аспектах прогнозирования атак, а не на проверке соответствия уже внедренных мер защиты [2-6].

Для определения места и роли квалиметрической оценки в системе аудита безопасности КИИ необходимо провести анализ существующих нормативно-методических подходов, принятых в Российской Федерации и в международной практике. В мировой практике сложилась устойчивая трехуровневая иерархия документов в области обеспечения информационной безопасности (ИБ) критически важных объектов. Стратегический уровень представлен такими документами, как: NIST Cybersecurity Framework (CSF) версии 2.0, COBIT. Их отличительной чертой является ориентация на желаемые исходы (outcomes) деятельности по обеспечению безопасности, а не на жесткую регламентацию конкретных технических действий.

Схожую целевую функцию в российском правовом поле выполняют Доктрина информационной безопасности и 187-ФЗ, однако они формулируют преимущественно императивные установки и принципы, оставляя детализацию на откуп подзаконным актам.

Процессный уровень в зарубежных подходах базируется на стандартах менеджмента (ISO/IEC 27001) и моделях оценки зрелости (Capability Maturity Model Integration – СММИ). Данный уровень предполагает не просто проверку наличия средств защиты, но и оценку качества управленческих процедур, их повторяемости и документированности.

Российским аналогом здесь выступают меры, закрепленные в приказах ФСТЭК России. Однако если СММИ предлагает четко градуированную шкалу зрелости (от начального до оптимизирующего уровня), то в отечественных нормативных актах оценка организационных мер носит преимущественно бинарный характер («наличие / отсутствие»).

Операционный (технический) уровень демонстрирует наибольшую степень корреляции между российскими и международными подходами.

Детализированные каталоги контролей, содержащиеся в NIST SP 800-53 и серии стандартов IEC 62443 (для автоматизированных систем управления технологическими процессами), по составу и глубине проработки во многом сопоставимы с мерами защиты, перечисленными в приказах ФСТЭК России. Это свидетельствует о том, что на уровне конкретных технических решений российская регуляторика находится в русле общемировых тенденций.

Принципиальное расхождение, имеющее определяющее значение обнаруживается на метрическом уровне. Международная практика уже перешла к обязательному измерению эффективности реализованных мер. Директива Европейского союза NIS2 прямо предписывает субъектам КИИ использовать метрики реагирования, показатели покрытия активов системами мониторинга и количественную оценку рисков (CRQ – Cyber Risk Quantification). Стандарт ISO/IEC 27004 предоставляет методологическую основу для разработки таких метрик и их интеграции в процессы принятия управленческих решений.

В российской нормативной базе аналогичные требования отсутствуют. Формулировки приказов ФСТЭК России остаются преимущественно качественными («должен осуществляться контроль», «должны применяться меры»), а методика проверки, используемая контролирующими органами, де-факто сводится к экспертной оценке соответствия, результаты которой трудно сопоставлять между различными объектами и периодами времени. Традиционный подход к аудиту ИБ в российской практике базируется на логике: проверяемое требование либо выполнено, либо не выполнено. Такой подход, будучи удобным для фиксации факта нарушения, оказывается недостаточным для решения задач стратегического управления защищенностью. Он не позволяет ответить на вопросы о том, насколько полно и качественно реализована та или иная мера, какова динамика состояния системы защиты во времени и, наконец, насколько один субъект КИИ отличается от другого по реальному уровню противодействия угрозам.

Квалиметрия – это научная дисциплина, изучающая методологию количественного оценивания качества объектов любой природы. Ключевой особенностью квалиметрического подхода является переход от констатации наличия или отсутствия отдельных свойств к измерению степени выраженности этих свойств в некоторой шкале.

Специфика оценки качества защищенности КИИ заключается в многоаспектности. Система защиты информации представляет собой сложный организационно-технический комплекс, эффективность которого зависит не только от исправности средств защиты, но и от зрелости процессов управления инцидентами, квалификации персонала и полноты внутренних нормативных документов.

Методика квалиметрической оценки должна обеспечивать учет вклада каждой из перечисленных составляющих в интегральную характеристику качества. Для обеспечения практической применимости квалиметрического подхода в условиях действующего нормативного регулирования предлагается двухуровневая модель интерпретации результатов аудита, синтезирующая обязательные требования регулятора с лучшими мировыми практиками оценки зрелости процессов.

Уровень 1. Базовый гигиенический минимум (Security Baseline). Данный уровень отвечает на принципиальный вопрос: создан ли у субъекта КИИ минимально необходимый фундамент защиты, требуемый законодательством? Содержательно он представляет собой проверку выполнения обязательных мер, перечисленных в соответствующих приказах ФСТЭК России. Оценка на этом уровне сохраняет бинарный характер («соответствует / не соответствует») в отношении каждого отдельного требования, однако итогом является не просто перечень замечаний, а агрегированный показатель (доля выполненных требований от общего числа обязательных для данной категории). Достижение установленного порогового значения (например, 95% выполнения базовых мер) является необходимым, но не достаточным условием для признания системы защиты эффективной.

Статистика проверок ФСТЭК России за 2025 год, согласно которой лишь 36% субъектов КИИ подтвердили минимальный уровень защищенности, наглядно демонстрирует, что проблема несоблюдения даже базовой «гигиены» стоит чрезвычайно остро. Внедрение единой метрики выполнения гигиенического минимума позволит регулятору и самим субъектам КИИ объективизировать картину и сконцентрировать усилия на тех направлениях, где отставание наиболее критично.

Уровень 2. Оценка зрелости процессов обеспечения ИБ. Второй уровень интерпретации ориентирован на оценку качества реализации тех мер, которые признаны выполненными на первом уровне. Он базируется на адаптации модели зрелости процессов СММИ к доменам (функциональным областям) защиты КИИ. В

качестве доменов, следуя логике NIST Cybersecurity Framework и одновременно учитывая структуру мер в приказах ФСТЭК России, предлагается выделить пять ключевых процессов:

- идентификация (Identify). Инвентаризации активов, категорирования объектов и оценки рисков;
- защита (Protect) – реализация технических и организационных мер по предотвращению реализации угроз (управление доступом, антивирусная защита, контроль целостности и т.д.);
- обнаружение (Detect) – процессы мониторинга событий безопасности, выявления аномалий и компьютерных атак;
- реагирование (Respond) – процессы обработки инцидентов, реагирования и оповещения, взаимодействия с ГосСОПКА;
- восстановление (Recover) – процессы резервного копирования, планирования восстановления и обеспечения непрерывности функционирования.

Каждому из пяти доменов разрабатывается шкала зрелости, градуированная по аналогии с классической моделью CMMI. Для обеспечения сопоставимости результатов аудитов различных субъектов КИИ и возможности отслеживания динамики состояния защищенности во времени необходимо установить единые принципы построения оценочных шкал и правила агрегирования частных показателей в интегральную оценку.

В качестве базовой шкалы предлагается использовать порядковую шкалу зрелости с диапазоном значений. Выбор порядковой шкалы обусловлен ее интуитивной понятностью как для технических специалистов, так и для руководства, а также возможностью непротиворечивого сопоставления с международными аналогами (CMMI, NIST CSF Tiers). При этом важно подчеркнуть, что переход к количественной оценке не означает полного устранения субъективного фактора – экспертное суждение аудитора остается необходимым элементом процедуры.

Задача квалитметрии состоит не в замене эксперта алгоритмом, а в структурировании и унификации процесса вынесения экспертного суждения. Агрегирование частных оценок зрелости по отдельным доменам в интегральный показатель защищенности осуществляется на основе принципа аддитивности с учетом весовых коэффициентов. Весовые коэффициенты отражают относительную важность каждого домена для обеспечения защищенности. Набор весовых коэффициентов может быть установлен экспертным путем с привлечением специалистов ФСТЭК России и отраслевых регуляторов либо определен на основе статистического анализа данных о реализованных инцидентах безопасности в разрезе нарушенных доменов. В любом случае фиксация весовых коэффициентов в методике обеспечивает единообразие расчетов и устраняет возможность манипулирования итоговой оценкой за счет произвольного выбора значимости тех или иных мер.

Итоговый интегральный показатель защищенности, выраженный в баллах от 0 до 5 (или в процентах от максимально возможного значения), представляет собой свертку оценок зрелости по всем пяти доменам.

Полученное значение интерпретируется в контексте двухуровневой модели: значение ниже установленного порога (например, 2,0 балла) свидетельствует о невыполнении базового гигиенического минимума и требует немедленных корректирующих действий; значение в диапазоне от 2,0 до 3,5 баллов соответствует приемлемому уровню защищенности с наличием резервов для совершенствования; значения выше 3,5 баллов характеризуют высокую степень зрелости процессов ИБ, сопоставимую с лучшими мировыми практиками.

Предложенная модель позволяет количественно охарактеризовать качество реализации защитных мер. Тем самым преодолевается методологический разрыв, выявленный в ходе сравнительного анализа отечественного и международного регулирования. Квалитметрическая оценка, несмотря на формализацию процедуры, не устраняет полностью фактор субъективности. Экспертное суждение аудитора остается необходимым элементом при присвоении баллов по шкале зрелости, особенно в пограничных случаях. Снижение влияния субъективного фактора возможно за счет детальной проработки критериев для каждого уровня зрелости, а также путем привлечения к аудиту нескольких независимых экспертов с последующим усреднением оценок.

Другим ограничением является необходимость адаптации весовых коэффициентов доменов к специфике конкретных отраслей КИИ, что требует проведения дополнительных экспертных сессий с участием отраслевых специалистов.

Перспективы дальнейших исследований связаны с разработкой детализированных критериев оценки зрелости для каждого из пяти доменов применительно к различным типам объектов КИИ; гармонизацией предложенной методики с подходами к оценке защищенности, разрабатываемыми в рамках международного сотрудничества по линии БРИКС и ЕАЭС.

Резюмируя изложенное, следует, что внедрение квалитметрической оценки в практику аудита субъектов КИИ способно качественно повысить объективность контрольных процедур, создать стимулы для

непрерывного совершенствования систем защиты и, в конечном счете, укрепить устойчивость КИИ в условиях, нарастающих киберугроз.

Литература

1. Доклад ФСТЭК России на Национальном форуме по кибербезопасности «Инфофорум 2026». – URL: <https://infoforum.ru/smi-o-nas/infoforum-2026-podvel-itogi-i-oboznachil-kljuchevye-kiberriski> (дата обращения: 21.04.2026).
2. Вульфин А.М. «Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных. – URL: <https://www.dissercat.com/content/modeli-i-metody-kompleksnoiotsenki-riskov-bezopasnosti-obekтов-kriticheskoi-informatsionnoi> (дата обращения: 21.04.2026).
3. Dushkin A.V., Goncharov N.I., Goncharov I.V., Parinov P.A. Modeling of Information Processes for Modern Information System Security Assessment // 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2019, p.p. 1758-1763. – DOI: 10.1109/EIConRus.2019.8656828. – Электронные данные. Режим доступа: URL: <https://ieeexplore.ieee.org/document/8656828> (дата обращения: 21.04.2026).
4. Kochedykov S.S., Grechishnikov E.V., Dushkin A.V., Orlova D.E. The mathematical model of cyber attacks on the critical information system. Journal of Physics: Conference Series, Voronezh. Vol. 1202. Voronezh: Institute of Physics Publishing, 2019. Pp. 12013. DOI 10.1088/1742-6596/1202/1/012013.
5. Лившиц И.И. «Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами» диссертация доктора технических наук: 05.13.19 / Лившиц Илья Иосифович. – Санкт-Петербург: СПИИРАН, 2018. – 407 с.
6. Макаренко С.И., Смирнов Г.Е. Модель аудита защищенности объекта критической информационной инфраструктуры тестовыми информационно-техническими воздействиями // Труды учебных заведений связи. – 2021. – №1. – С. 23-46.

APPLICATION OF QUALITICAL ASSESSMENT IN CONDUCTING AN INFORMATION SECURITY AUDIT OF A CRITICAL INFORMATION INFRASTRUCTURE ENTITY

postgr. Nilov N.A., prof. Dushkin A.V.

National Research University of Electronic Technology

This article addresses the discrepancy between the growing number of regulatory requirements for the protection of Russia's critical information infrastructure (CII) and the lack of objective methods for quantitatively assessing their implementation. A comparative analysis of domestic regulations and international standards reveals a fundamental methodological discrepancy at the metric level: Russian regulations rely on qualitative, binary assessments, while global practice is shifting toward quantitative measurement of process efficiency and maturity. A two-tier qualimetric assessment model is proposed that synthesizes mandatory regulatory requirements with CMMI principles. The model includes the calculation of a basic "hygienic minimum" performance indicator and an integrated maturity assessment across five domains (identification, protection, detection, response, and recovery) based on an ordinal scale and weighting factors. Implementation of the proposed approach helps overcome this discrepancy, objectify audit results, and create incentives for the continuous improvement of CII protection systems in the face of escalating cyber threats.



РАЗРАБОТКА МЕТОДИКИ ВЫЯВЛЕНИЯ ЗАКЛАДОЧНЫХ УСТРОЙСТВ, ПОСТРОЕННЫХ НА БАЗЕ СРЕДСТВ СОТОВОЙ СВЯЗИ, С ИСПОЛЬЗОВАНИЕМ ИМИТАТОРА БАЗОВОЙ СТАНЦИИ

студ. Орлов П.А., д.т.н. доц. Щербаков В.А.

Национальный исследовательский университет «МИЭТ»

Целью исследований является разработка программно-аппаратного комплекса выявления закладочных устройств, построенных на базе средств сотовой связи, с использованием имитатора базовой станции.

В работе разработан экспериментальный программно-аппаратный комплекс, реализующий функции имитатора базовой станции на базе мобильного телефона Motorola C118 и программного обеспечения OsmocomBB. Проведённые экспериментальные исследования подтвердили возможность регистрации идентификаторов подключённых устройств и показали работоспособность предложенного решения в условиях контролируемого помещения.

Полученные результаты демонстрируют возможность применения разработанной методики при проведении специальных обследований и мероприятий по технической защите информации для повышения эффективности выявления закладочных устройств, использующих каналы сотовой связи.

Введение

В условиях стремительного развития телекоммуникационных технологий и повсеместного распространения мобильной связи существенно возросли риски утечки информации по техническим каналам. Особую угрозу представляют закладочные устройства, использующие инфраструктуру сотовых сетей, поскольку они обеспечивают скрытую и практически неограниченную по дальности передачу информации.

Современные средства негласного получения информации становятся всё более миниатюрными, энергоэффективными и функциональными, что значительно усложняет их выявление.

В связи с этим задача повышения эффективности выявления закладочных устройств, функционирующих в сетях сотовой связи, является одной из приоритетных в области технической защиты информации.

Закладочные устройства данного класса обладают рядом принципиальных особенностей, отличающих их от традиционных радиозакладок. Ключевыми из них являются:

- неограниченная дальность использования
- использование стандартных протоколов связи, что маскирует работу устройств под легитимный трафик;
- наличие удалённого управления посредством SMS или голосовых вызовов;
- возможность работы в скрытых режимах (спящий режим, активация по событию, пакетная передача данных);
- высокая степень маскировки под бытовые и электронные устройства.

Указанные особенности существенно снижают эффективность традиционных методов радиоконтроля и требуют применения специализированных подходов к обнаружению.

Применяемые на практике методы выявления закладочных устройств, такие как радиомониторинг, спектральный анализ и нелинейная радиолокация не обеспечивают гарантированного обнаружения устройств, не позволяют однозначно идентифицировать функциональное назначение обнаруженного объекта, не обеспечивают необходимой полноты контроля в условиях высокой степени маскировки устройств.

Таким образом, существующие подходы не обеспечивают требуемой результативности обнаружения современных закладочных устройств, особенно при их скрытной работе в сетях сотовой связи.

С учётом выявленных ограничений актуальной является разработка новых методов обнаружения закладочных устройств, основанных на активном воздействии на их функционирование.

Одним из перспективных направлений является использование имитатора базовой станции сотовой связи, позволяющего инициировать взаимодействие с абонентскими устройствами и выявлять присутствие несанкционированных средств связи по их реакциям на сетевые воздействия.

В рамках данной работы ставится задача разработки методики выявления закладочных устройств, функционирующих в сетях сотовой связи, с использованием имитатора базовой станции, обеспечивающей: повышение вероятности обнаружения устройств, работающих в скрытых режимах; выявление несанкционированных SIM-устройств; возможность локализации источников сигнала.

Целью работы является разработка программно-аппаратного комплекса выявления закладочных устройств, построенных на базе средств сотовой связи, с использованием имитатора базовой станции.

Основная часть

Закладочные устройства, используемые для негласного съёма информации, представляют собой технические средства, предназначенные для скрытого перехвата и передачи данных по различным каналам связи [1].

Анализ объекта выявления показывает, что закладочные устройства подразделяются на устройства акустического съёма информации, телефонные закладки, а также комбинированные решения, обеспечивающие перехват как акустической информации помещения, так и сигналов в линиях связи [1]. При этом передача перехваченной информации может осуществляться по различным каналам, включая радиоканал и сети связи, что определяет место установки устройства и его конструктивные особенности. Особое место занимают устройства, маскируемые под бытовую и электронную технику, что существенно осложняет их обнаружение при проведении традиционных мероприятий контроля.

Принцип действия GSM-закладок основан на использовании стандартных механизмов функционирования абонентских устройств сотовых сетей. В состав таких устройств входят радиомодуль, SIM-карта, управляющий микроконтроллер и периферийные элементы, обеспечивающие съём информации. После включения устройство регистрируется в сети оператора, переходит в режим ожидания и активируется при наступлении заданных условий, таких как входящий вызов, получение SMS-команды или фиксация акустического сигнала. Передача информации осуществляется через голосовые каналы или посредством пакетной передачи данных.

Основными особенностями закладочных устройств данного типа являются использование легитимной телекоммуникационной инфраструктуры, наличие уникальных идентификаторов (IMSI и IMEI), возможность удалённого управления, а также реализация режимов скрытной работы, включая энергосберегающие режимы и активацию по событию [2]. Импульсный характер радиообмена и использование стандартных частотных диапазонов затрудняют их выявление средствами радиоконтроля.

Традиционные методы обнаружения закладочных устройств, такие как радиомониторинг, спектральный анализ и нелинейная радиолокация, обладают ограниченной эффективностью в отношении устройств на базе сотовой связи. Радиомониторинг позволяет фиксировать только активные сеансы передачи, что не обеспечивает выявления устройств, функционирующих в режиме ожидания. Спектральный анализ осложняется необходимостью выделения сигнала на фоне легитимного трафика. Нелинейные локаторы, в свою очередь, выявляют наличие электронной компонентной базы, но не позволяют определить функциональное назначение обнаруженного объекта. Указанные ограничения обуславливают необходимость разработки активных методов выявления.

Теоретической основой предлагаемого подхода является использование имитатора базовой станции сотовой связи, обеспечивающего взаимодействие с абонентскими устройствами в контролируемой зоне. Известно, что любое устройство сотовой связи периодически выполняет процедуры поиска сети, регистрации и обмена служебной информацией. При появлении в зоне действия базовой станции с более приоритетными параметрами устройство инициирует процедуру переподключения. Данное свойство позволяет организовать контролируемую среду, в которой все активные абонентские устройства регистрируются в имитаторе базовой станции.

В рамках предлагаемой методики имитатор базовой станции формирует зону радиопокрытия с заданными параметрами, обеспечивающими привлечение абонентских устройств. В процессе регистрации осуществляется сбор идентификационных данных, включая IMSI и IMEI. Полученные данные анализируются с целью выявления устройств, не входящих в перечень легитимных. Дополнительно может осуществляться анализ поведенческих характеристик устройств, а также их локализация на основе измерения уровня сигнала [2].

Для реализации данного подхода разработана структура комплекса выявления, включающая аппаратную и программную части. Аппаратная часть содержит имитатор базовой станции, радиочастотный тракт, включающий антенны и усилители, а также вычислительный модуль. Программная часть включает модули управления базовой станцией, сбора и хранения идентификационных данных, аналитический модуль и интерфейс оператора. Функционально комплекс обеспечивает формирование зоны покрытия, регистрацию устройств, сбор и анализ данных, а также визуализацию результатов.

В процессе передачи сигнала цифровой поток формируется центральным процессором, после чего выполняется его преобразование в аналоговый сигнал, усиление и передача через антенну. Прием сигнала выполняется в обратном порядке и сопровождается его фильтрацией, аналого-цифровым преобразованием и последующей программной обработкой (схема представлена на рисунке 1) [3].

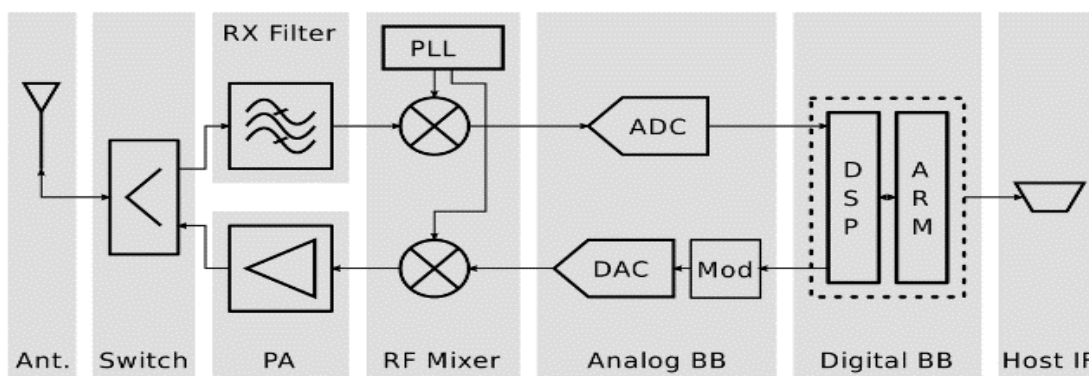


Рисунок 1 – Структурная схема имитатора базовой станции

Алгоритм функционирования комплекса включает несколько этапов. На первом этапе осуществляется развертывание комплекса и настройка параметров имитатора базовой станции. Далее производится активация системы и привлечение абонентских устройств. На этапе регистрации выполняется сбор идентификаторов устройств и формирование их перечня. Полученные данные сопоставляются с базой доверенных устройств, в результате чего выявляются подозрительные объекты.

Разработан экспериментальный программно-аппаратный комплекс для имитации базовой станции GSM. В качестве радиомодуля использован мобильный телефон Motorola C118 с сигнальным процессором Calypso, поддерживаемый проектом OsmocomBB. Управление модулем осуществляется через ПК с помощью интерфейсного преобразователя USB-TTL и программного обеспечения AutoCalypsoBTS. Операционная система DragonOS обеспечивает работу комплекса, который создаёт локальную GSM-сеть и управляет её параметрами (рисунок 2).

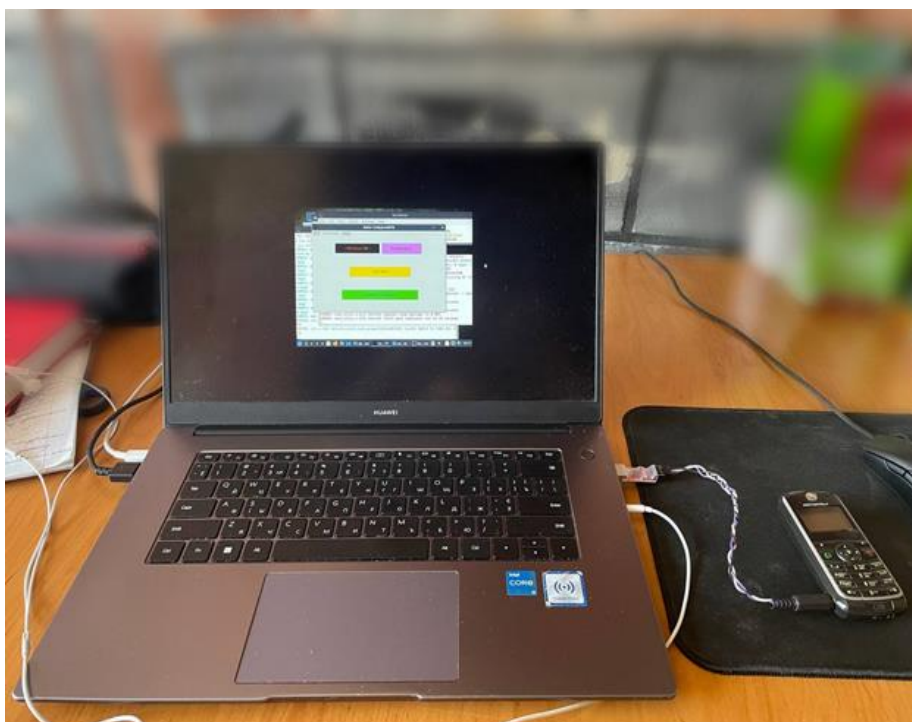


Рисунок 2 – Разработанный имитатор базовой станции

Экспериментальная проверка работоспособности комплекса проводилась в условиях помещения с тестовым устройством, в качестве которого использовался смартфон Xiaomi Redmi Note 11S. В ходе эксперимента обеспечено успешное привлечение устройства в зоне действия имитатора базовой станции, так как сигнал имитатора более мощный, чем сигнал базовой станции оператора (рисунок 3). Идентификационные данные были получены в полном объёме, при этом тестовое устройство было выделено (рисунок 4).



Рисунок 3 – Сравнение мощностей GSM-сигнала имитатора и базовой станции сотового оператора

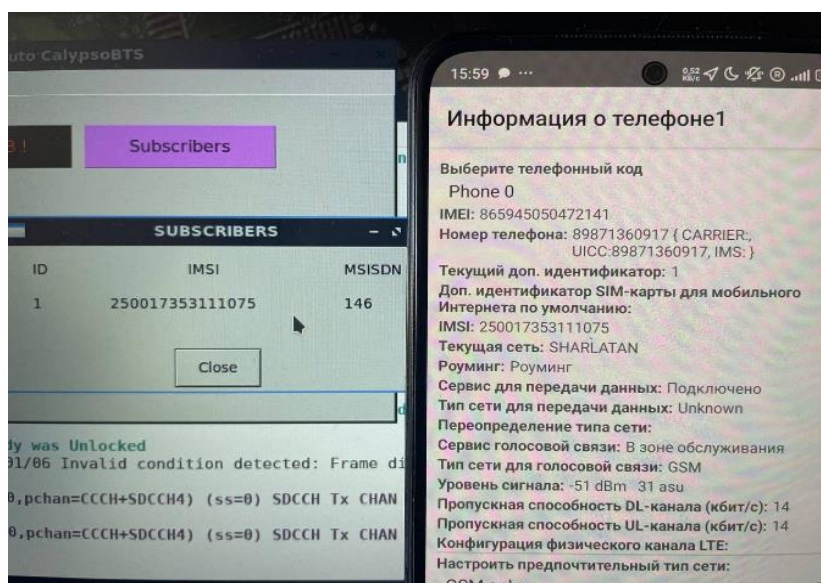


Рисунок 4 – Разработанный имитатор базовой станции

Полученные результаты свидетельствуют о высокой эффективности предложенного метода, в том числе при выявлении устройств, функционирующих в скрытных режимах. В отличие от пассивных методов, использование имитатора базовой станции позволяет инициировать взаимодействие с устройствами, что существенно повышает вероятность их обнаружения. Например, возможность отправки сообщений для дальнейшей пеленгации закладочного устройства (рисунок 5)

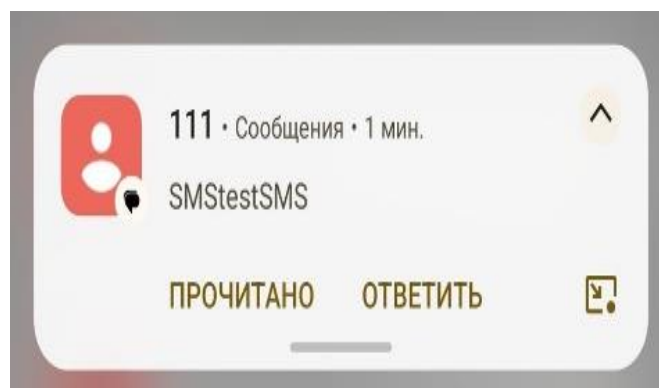


Рисунок 5 – Тестирование функции отправки SMS

Анализ результатов

Разработанный комплекс выявления закладочных устройств на базе средств сотовой связи с использованием имитатора базовой станции обладает высокой практической значимостью и эффективностью при решении задач технической защиты информации.

Данный комплекс может применяться при проведении специального обследования для обнаружения скрытых закладочных устройств в защищаемом помещении, а также при проведении специальной проверки, что позволяет значительно повысить эффективность и сократить время выполнения работ. Использование активного метода обеспечивает выявление устройств независимо от режима их работы, включая скрытые состояния.

К основным практическим преимуществам комплекса относятся:

- высокая вероятность обнаружения за счёт принудительной регистрации устройств;
- возможность идентификации по уникальным параметрам (IMSI, IMEI).

Для эффективного применения комплекса рекомендуется:

- использовать его в составе комплексных мероприятий совместно с другими средствами выявления;
- использование генераторов шума для эффективного присоединения закладочного устройства к имитатору базовой станции;
- пеленгование для дальнейшей локализации и выявления закладочного устройства;
- подтверждать результаты технического выявления физическим обследованием.

Литература

1. Хорев Анатолий Анатольевич Классификация электронных устройств перехвата информации // Спецтехника и связь. 2009. №1. URL: <https://cyberleninka.ru/article/n/klassifikatsiya-elektronnyh-ustroystv-perehvata-informatsii> (дата обращения: 17.03.2026).
2. GSM-ловушки: ещё один привет от Большого Брата [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/companies/securitycode/articles/280886/>, свободный (Дата обращения: 17.03.2026).
3. Уязвимости 2G [Электронный ресурс]. – Режим доступа: <https://radio-secure.ru/secure/2g#e>, свободный (Дата обращения: 17.03.2026).

DEVELOPMENT OF A METHODOLOGY FOR IDENTIFYING STORAGE DEVICES BASED ON CELLULAR COMMUNICATIONS USING A BASE STATION SIMULATOR

stud. Orlov P.A., Dr. Sci. Assoc. Prof. Shcherbakov V.A.

National Research University of Electronic Technology

The purpose of the research is to develop a hardware and software complex for detecting laying devices based on cellular communications using a base station simulator.

An experimental hardware and software package has been developed that implements the functions of a base station simulator based on a Motorola C118 mobile phone and OsmocomBB software. The conducted experimental studies confirmed the possibility of registering the identifiers of connected devices and showed the operability of the proposed solution in a controlled environment.

The results obtained demonstrate the possibility of using the developed methodology in conducting special surveys and measures for the technical protection of information to increase the effectiveness of detecting bookmarks using cellular communication channels.



СПОСОБ ИДЕНТИФИКАЦИИ РАДИОСИГНАЛОВ ЗАКЛАДНЫХ УСТРОЙСТВ, ПОСТРОЕННЫХ НА БАЗЕ СИСТЕМ БЕСПРОВОДНОГО ДОСТУПА, ПУТЕМ АЛИЗА ОГИБАЮЩИХ ИХ СПЕКТРОВ

студ. Кандидатов Р.А., к.т.н. Панцыр Р.Я., студ. Парфенов А.А.

Национальный исследовательский университет «МИЭТ»

В статье рассматривается проблематика оперативного обнаружения электронных устройств негласного получения информации в условиях невозможности их демодуляции и декодирования. Предложен способ статистического накопления и идентификации радиосигналов по огибающей спектра без необходимости декодирования передаваемых данных. На примере стандарта DECT описан алгоритм выделения идеализированного контура сигнала с последующим применением библиотек компьютерного зрения для автоматизированной трассировки и классификации излучений.

1.

2. Введение

В современном мире с развитием беспроводных систем связи стоит важный вопрос идентификации новых появляющихся средств. Емкости современных каналов связи при огромном количестве устройств, требующих дистанционного управления и телеметрии, уже недостаточно. В связи с этим будут стремительно развиваться другие технологии обмена данными. С развитием данных технологий, в том числе для скрытия факта передачи информации, злоумышленники будут пользоваться модулями легальных средств передачи данных. Это делается для того, чтобы сделать сигналы от закладного устройства (ЗУ) неразличимыми от сигналов легальных средств.

Вместе с тем достаточно большое внимание уделяется закрытию каналов связи. При условии применения шифрования используемые до сих пор методы демодуляции радиосигнала и декодирования видеосигнала для получения открытой информации становятся все более трудными, а зачастую и невозможными. Отсюда следует вывод, что требуются новые методы и способы идентификации радиоизлучений. Полное техническое и программное описание новых стандартов доходит до широкой публики через несколько лет и представляет собой сотни страниц инженерного текста с неоднозначным переводом. Таким образом, нужно разработать способ оперативной идентификации сигналов без их декодирования.

1. Способ оперативной идентификации сигналов по огибающей спектра

В свободных каналах могут быть использованы сигналы, визуально похожие по спектру, но не являющиеся одним стандартом беспроводной связи. Человек глазами не способен достоверно идентифицировать такой сигнал на огибающей спектра, из-за высокой скорости передачи и большого количества параметров: центральные частоты, ширина полос, форма спектра.

Обнаружение и идентификация радиосигналов основаны на получении спектра и огибающей спектра с последующим анализом обнаруженных сигналов. Современные комплексы радиоконтроля позволяют проводить цифровой анализ множества стандартов, таких как Bluetooth, Wi-Fi, ZigBee и DECT, осуществляя перехват идентификационной информации из открытой части пакетов. Однако при закрытой информации или применении методов противодействия, таких как смещение центральных частот в сетке каналов радиозакладки, традиционные методы неэффективны.

Поскольку маскирующим признаком в данном случае остается само электромагнитное излучение и его форма, одним из наиболее применяемых способов является анализ огибающей спектра сигнала. Для оперативной идентификации сигналов предлагается следующий способ. Изначально осуществляется получение приема-передающего устройства, на основе которого могут быть построены ЗУ, для проведения исследования и статистического накопления его сигналов. Далее производится построение идеализированного спектра сигнала. На следующем этапе производится выделение основных параметров сигнала: центральных частот каналов, ширины полос, распределения спектральной плотности и формы огибающей. Завершающим этапом является идентификация сигнала и автоматическая обработка в виде разработки математического алгоритма или использование уже известных библиотек с настраиваемыми параметрами для идентификации сигнала, что позволяет проводить сканирование спектра, автоматическую трассировку усредненной линии и быструю идентификацию [1].

2. Практическая реализация алгоритма и описание работы на примере стандарта DECT.

Стандарт DECT представляет собой систему беспроводного доступа, работающую в выделенном диапазоне частот 1880 – 1900 МГц и использующую временное разделение каналов. Примечательно, что сигналы этого стандарта характеризуются достаточно стабильной полосой частот и типовой формой

спектральной, огибающей [4]. Именно поэтому он оказывается удобным объектом для анализа и построения эталонных моделей.

Первый этап алгоритма начинается с загрузки спектральной линии и её преобразования. Изображение переводится в градации серого, чтобы убрать влияние цветовой составляющей и сосредоточиться исключительно на распределении спектра с помощью библиотеки OpenCV [3]. Затем применяется пороговая бинаризация с настраиваемым уровнем чувствительности, в результате чего выделяется область, соответствующая основному спектральному контуру сигнала. Такой подход позволяет подавить фоновый шум и оставить только действительно информативную часть спектра.

После бинаризации выполняется поиск контуров. Среди них выбирается крупнейший по площади – он соответствует предполагаемой огибающей спектра. Для этого контура определяется ограничивающая область, внутри которой и проводится дальнейший анализ. Чтобы обеспечить устойчивость к изменению положения и масштаба сигнала, выделенная область нормализуется и приводится к фиксированному размеру. Это даёт возможность корректно сопоставлять спектры, полученные в разных условиях наблюдения.

Далее оценивается шумовая составляющая сигнала. Здесь используется оператор Лапласа, позволяющий вычислить дисперсию высокочастотных компонентов изображения. Полученное значение отражает уровень зашумлённости спектра и применяется как один из критериев достоверности идентификации. Сравнение исследуемого сигнала с эталоном выполняется методом поточечного процентного сопоставления на основе анализа формы выделенного контура. Дополнительно применяются инвариантные моменты Ху, которые позволяют количественно оценить сходство геометрии объектов независимо от их масштаба и ориентации. На основе этих данных формируется коэффициент сходства формы огибающей. Параллельно вычисляется коэффициент спектральной чистоты как отношение дисперсий шума эталонного и исследуемого сигналов. Вероятность идентификации формируется как комбинация этих двух критериев. При этом больший вес может быть отдан параметру, характеризующему устойчивость сигнала к шуму. Такое объединение признаков повышает надёжность распознавания в условиях реального радиоэфира, где форма спектра нередко искажается. Решение о принадлежности сигнала к заданному стандарту принимается путём сравнения итоговой вероятности с пороговым значением, определяемым экспериментально. При превышении установленного порога сигнал считается идентифицированным, в противном случае он отклоняется как не соответствующий эталону.

Блок-схема алгоритма программного обеспечения (ПО) представлена на рисунке 1.

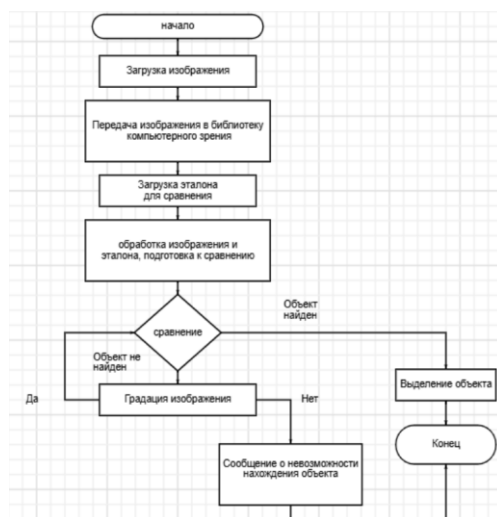


Рисунок 1 – Блок-схема алгоритма ПО

Для того чтобы алгоритм мог стабильно узнавать сигнал в условиях шумов, необходимо накопить статистику. На рисунке 2 представлен внешний вид типовых огибающих спектра DECT, полученного с помощью специализированного программно-аппаратного комплекса, разработанного для выявления средств беспроводного доступа. А на рисунке 3 представлена эталонная огибающая спектра сигнала стандарта DECT.

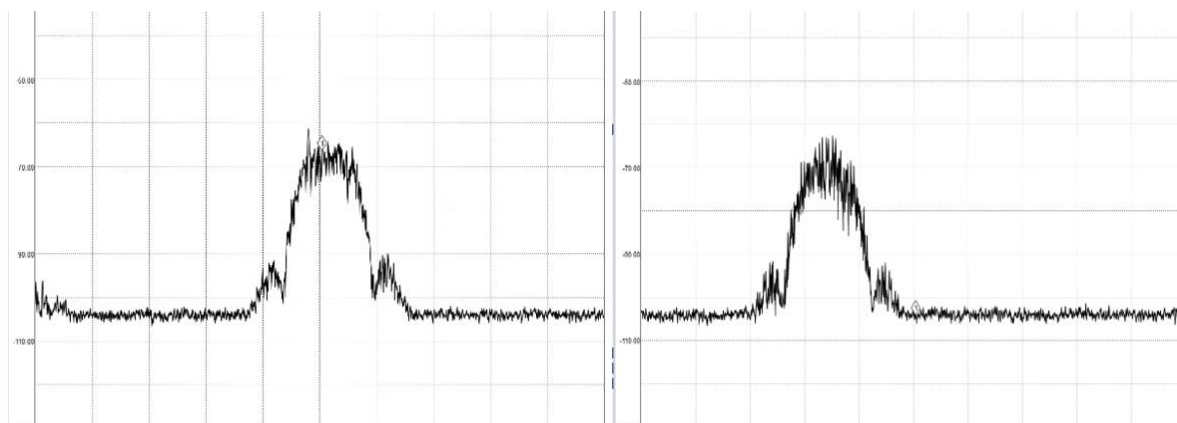


Рисунок 2 – Внешний вид типовых огибающих спектра

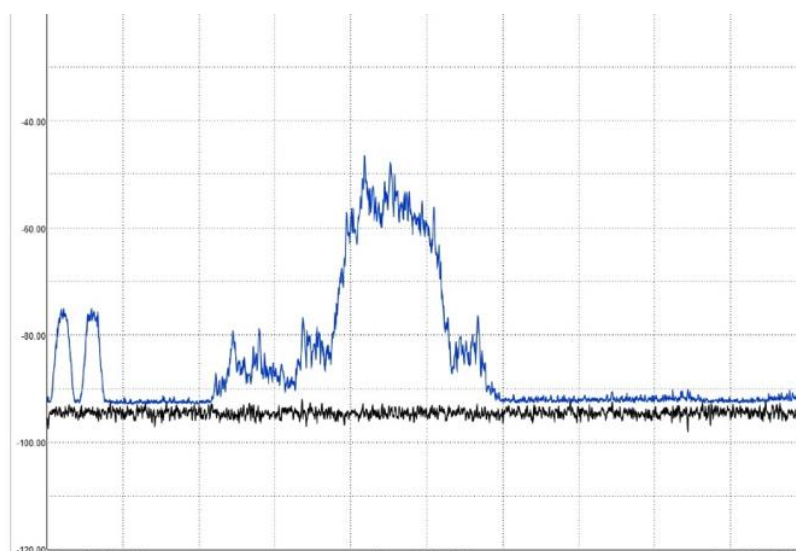


Рисунок 3 – Эталонная огибающая спектра сигнала стандарта DECT, сформированная по результатам статистического накопления

Программное сканирование спектра и использование методов дисперсионного анализа позволяют надежно идентифицировать искомый сигнал и отсеивать схожие по форме помехи на рисунке 4 представлен интерфейс разработанной программы. На рисунке 5 представлены результаты наложения эталонной огибающей на реальный сигнала DECT, полученных в разные периоды времени.

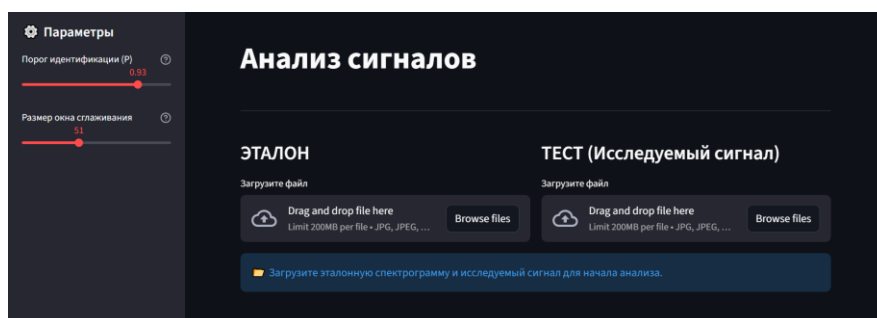


Рисунок 4 – Интерфейс программы

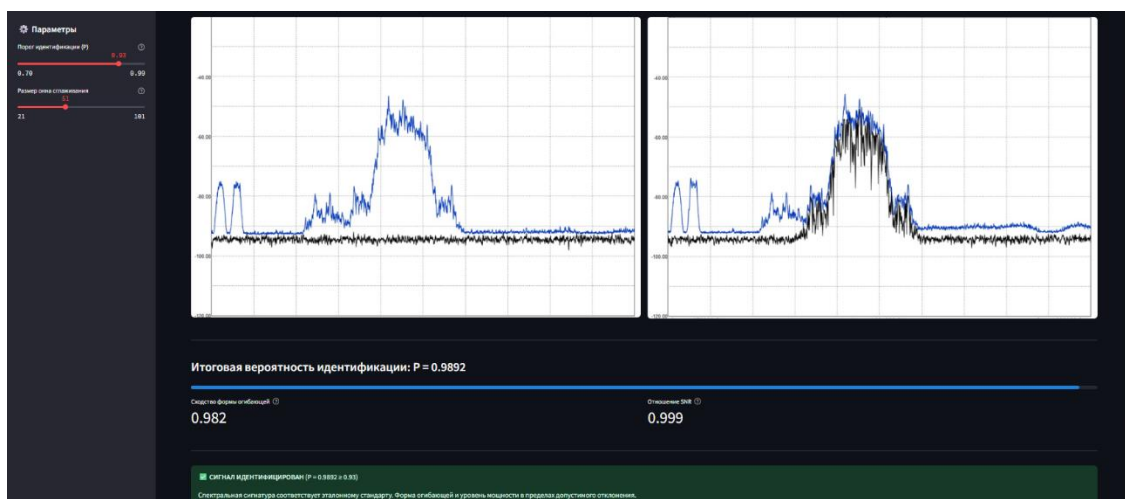


Рисунок 5 – Результат успешной идентификации при совпадении огибающих

Преднамеренное использование сигналов других стандартов, которые внешне повторяют огибающую сигнала DECT может является проблемой.

На рисунке 6 показано сопоставление эталонной огибающей спектра DECT и сигнала с дельта-модуляцией. Несмотря на визуальное сходство, алгоритм всё же улавливает характерные расхождения в форме, огибающей.

В результате вероятность не дотягивает до порогового значения $P = 0,93$ полученного экспериментальным путем.

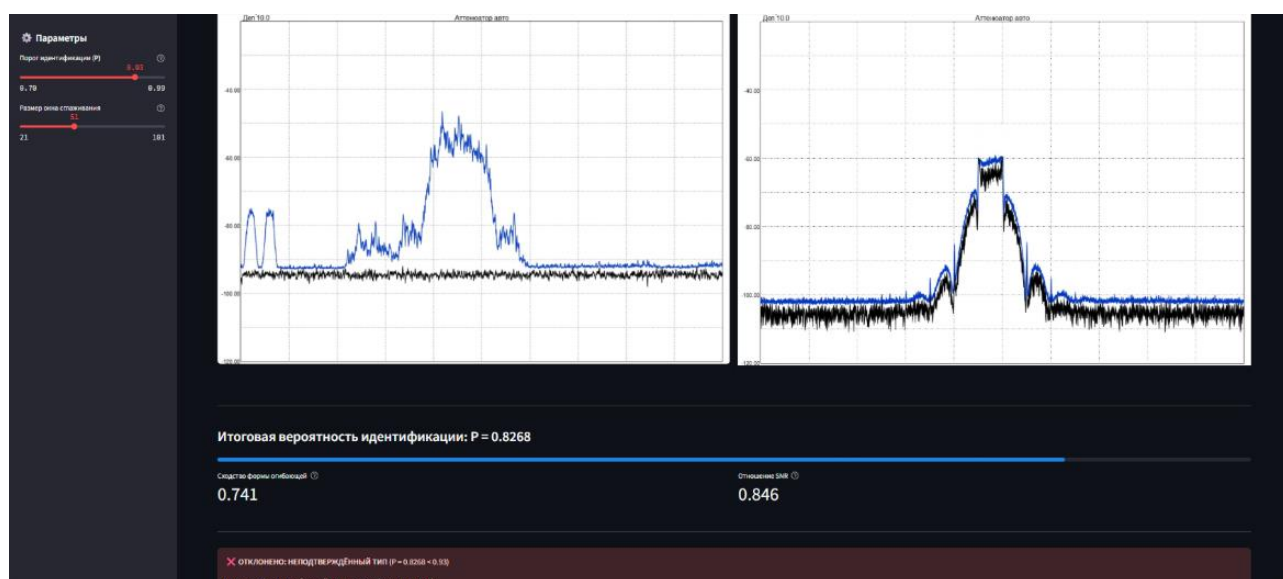


Рисунок 6 – Сравнение эталона огибающего спектра с сигналом дельта-модуляцией

Шумовые искажения – далеко не единственная проблема, ведь существует и другая угроза: намеренное использование сигналов иных стандартов, которые визуально напоминают огибающую сигнала DECT. Чтобы проверить, насколько наш алгоритм устойчив к таким случаям, обратимся к рисунку 7. Там показано сравнение эталонной огибающей спектра DECT с сигналом псевдослучайной перестройки рабочей частоты (ППРЧ).

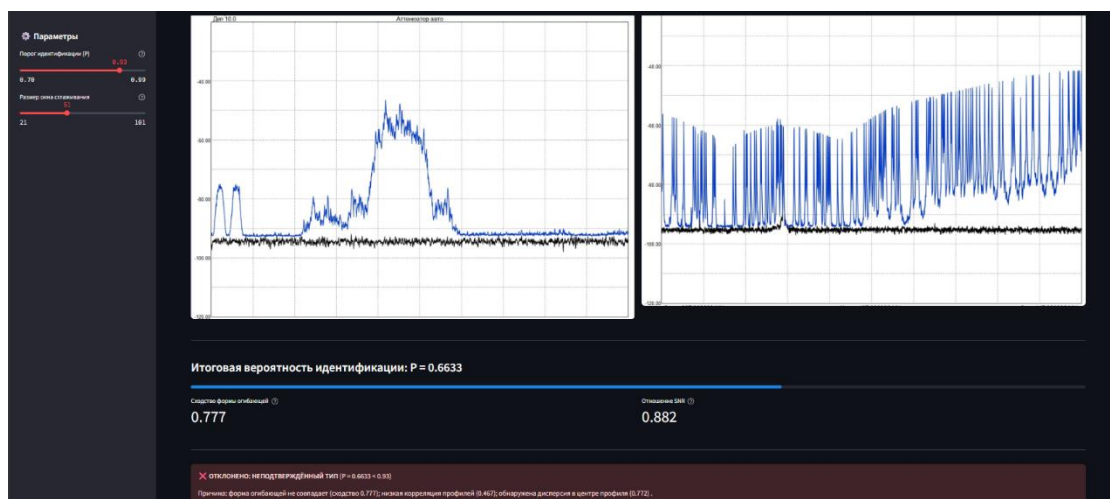


Рисунок 7 – Сравнение эталона огибающей спектра с сигналом псевдослучайной перестройки рабочей частоты

Заключение

Предложенный способ статистического накопления и анализа огибающей спектра позволяет проводить оперативную идентификацию радиосигналов без необходимости их демодуляции и декодирования. Важно, что такой подход обеспечивает устойчивость к шумам и вариациям условий передачи – и достигается это за счёт использования усреднённых спектральных характеристик, а также анализа формы сигнала. Стоит отметить, что именно сочетание этих факторов и даёт системе стабильность. Практическая значимость работы, что немаловажно, заключается в возможности применения предложенного подхода в системах радиомониторинга. В частности, для выявления закладных устройств, использующих легальные стандарты беспроводной связи.

Литература

1. Белый В.М. Эффективность информационных систем и информационных технологий: учебник / В.М. Белый, Р.В. Белый – Королев МО: ФТА.2013 г – 396 с.;
2. Хорев А.А. Теоретические основы оценки возможностей технических средств разведки Монография. – М.: МО РФ, 2000 г. – 255 с.;
3. Сайт библиотекой и документацией по OpenCV [Электронный ресурс]. – Режим доступа: <https://opencv.org/>;
4. Гондин Д.А. «Цифровая обработка сигналов средствами графических ускорителей» [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/tsifrovaya-obrabotka-signalov-sredstvami-graficheskikh-uskoriteley/viewer>;

A METHOD FOR IDENTIFYING RADIO SIGNALS OF EAVESDROPPING DEVICES BUILT ON THE BASIS OF WIRELESS ACCESS SYSTEMS BY ANALYZING THEIR SPECTRAL ENVELOPES

stud. Kandidatov R.A., Ph.D. Pantsyr R.Ya., stud. Parfenov A.A.

National Research University of Electronic Technology

This article examines the challenges of quickly detecting electronic devices for covert information acquisition when demodulation and decoding are impossible. A method for statistically accumulating and identifying radio signals based on their spectral envelope is proposed, eliminating the need to decode the transmitted data. Using the DECT standard as an example, an algorithm for extracting an idealized signal contour is described, followed by the use of computer vision libraries for automated tracing and.



ОСОБЕННОСТИ УПРАВЛЕНИЯ РЕСУРСАМИ ПРИ РАЗВИТИИ ЗАЩИЩЕННОСТИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

доц., к.т.н. Ерохин С.Д.¹, доц., к.т.н., Петухов А.Н.², к.т.н. Пилюгин П.Л.²

¹Московский технический университет связи и информатики

²Национальный исследовательский университет «МИЭТ»

Обсуждаются ресурсные аспекты управления информационной безопасностью, предполагающие динамическое развитие защитных возможностей в процессе функционирования. Это актуально для критических информационных инфраструктур, которым свойственна некоторая априорная неопределенность целевых параметров защищенности. Рассматриваются исключительные ситуации в отношении использования ресурсов на определенных этапах жизненного цикла. Показана необходимость многоаспектности критериев управления ресурсами и учета внутренней структуры ресурсов – реагирования и функционирования, а также связь типологии затрат и ресурсоемкости с характером развития защищенности – параметр, структура или сервис. Приведена схема формализации ограничений уровня защищенности и затрачиваемых ресурсов для используемой модели опасностей с учетом «неидентифицированного» остаточного риска. Показано, что асимптотическое управление не только повышает уровень защищенности, но и снижает «неидентифицированный» риск.

В настоящее время все большее распространение получают методы управления информационной безопасностью, предполагающие динамическое развитие защитных возможностей непосредственно в процессе функционирования информационной системы. В частности, это характерно для критических информационных инфраструктур, которым свойственна некоторая априорная неопределенность целевых параметров для достигаемого в процессе управления уровня защищенности [1]. Эта особенность критических инфраструктур затрудняет планирование ресурсов для обеспечения безопасности, и порождает естественные вопросы: а какова вообще может быть цена такого развития защищенности, можно ли этой ценой управлять, и есть ли возможность ее заплатить?

Управление ресурсами при развитии защищенности связано с решением некоторых методологических и отчасти формальных математических задач, постановка и выполнение которых требуют предварительных комментариев.

Основным первоначальным постулатом является утверждение, что любая деятельность по управлению информационной безопасностью непременно требует многоаспектных затрат ресурсов, как материальных, так и нематериальных. Независимо от базовой методологии управления – будь то асимптотический подход [2] или обеспечение допустимого риска [3], любой метод управления сопряжен с ресурсными расходами. В пределах этого, на первый взгляд тривиального, тезиса можно рассуждать только о том, что и как расходуется в качестве ресурса и как этим расходом управлять. Другими словами, принципиально не может быть методики управления безопасностью (в т.ч. развития защищенности) в условиях абсолютного отсутствия ресурсов, может быть только методика минимизации расходования, методика запаса (накопления) или резервирования (планирования, бюджетирования) ресурсов и т.п.

При этом, некоторые исключительные ситуации в отношении использования ресурсов могут рассматриваться на определенных этапах жизненного цикла критической информационной инфраструктуры. На этапе создания и внедрения системы защиты обычно есть возможность относительно гибко использовать необходимые ресурсы. В то же время, на этапе эксплуатации управление ресурсами ограничено более жесткими рамками. Тем не менее, для исключения экстраординарных последствий (возможность которых позволяет относить критическую инфраструктуру к категории значимых [4]) может быть предусмотрена методика «аварийного поведения», когда запасы и резервы исчерпаны (т.е. ресурсы полностью отсутствуют), а перспектива катастрофы реальна. Методически эта ситуация выходит за пределы тематики управления ресурсами в рамках обеспечения информационной безопасности и может рассматриваться с привлечением методов поддержания непрерывности информационной деятельности (бизнеса) [5].

Известно, что одной из фундаментальных проблем информационной безопасности является проблема метризации – привлечения объективных (неэкспертных) количественных мер оценивания защищенности. Наряду с этим самостоятельной задачей является исчисление ресурсов, используемых для реализации мер защиты, с учетом того, что таких ресурсов, как правило, может быть несколько их различных видов.

Структурно самая простая схема управления ресурсами сводит все к монетизации, т.е. рассматривает только один вид ресурса – экономический. В нашем случае возникают существенные ограничения для такого подхода. Во-первых, в этом случае проблема ограничения ресурса управления безопасностью переводится в класс исключительно экономических задач, в то время как уже на первоначальном этапе управления – категорировании критических инфраструктур, привлекается широкий круг «неэкономических» [4] критериев. Во-вторых, такая концепция требует построения экономических моделей для факторов и методов безопасности, что за пределами рискориентированного подхода затруднительно без субъективной экспертизы. Кроме того, даже для относительно простых методов, например, использования совокупной

стоимости владения, результаты существенно зависят от внешних факторов (например, от качества работы бухгалтерии).

Поэтому, нисколько не умаляя роль экономического аспекта, при оценке ресурсов следует рассматривать в качестве наиболее значимых собственно технические вопросы. Можно выделить два вида привлекаемых технических ресурсов:

- Ресурсы реагирования – вычислительные мощности (процессорная производительность, различные виды памяти, пропускная способность линий связи и т.п.), которые необходимы для реализации реакции на инцидент. В составе средств асимптотического управления безопасностью это материальная база транзакции корректировки мер защиты;
- Ресурсы функционирования – издержки вычислительных мощностей (снижение производительности, сокращение функциональности и т.п.), которые понесла защищаемая технология и инфраструктура. Это цена, которую «заплатил» защищаемый объект за повышение его защищенности.

Ресурсы этих видов во многом пересекаются, но это не одно и то же. Если ресурсы реагирования поддаются какому-то прогнозированию, то ресурсы функционирования, как правило, расходуются «по факту». Технические ресурсы труднее бюджетировать, нежели экономические, поэтому они играют основную роль при анализе ресурсных ограничений для непрогнозируемых транзакций асимптотического управления безопасностью.

Есть и другие виды издержек от оперативных корректировок, например, процедурные, когда вносятся изменения и теряется поддержка вендора, но они, как правило, монетизируются и вместе с такими регулярными статьями, как расходы на персонал, управляются в рамках экономических моделей.

Использование ресурсов для обеспечения текущего уровня безопасности носит статический и динамический характер. На этапе создания системы защиты расходы бюджетировются, и экономические, энергетические и технические ресурсы балансируются. Функциональность системы защиты статически соотносена с требуемым ресурсом, и реализуется при предоставлении этого ресурса.

В настоящее время, когда безопасность в большинстве случаев продолжает рассматриваться как затратный аспект деятельности, ее планомерному развитию предшествует планирование соответствующего ресурса, и по мере предоставления этого ресурса запланированное развитие безопасности реализуется. В частности, выполнение цикла Деминга-Шухарта [6] и процессы удержания нормативного уровня защищенности [1] осуществляются именно таким образом.

Для асимптотического управления ситуация иная, и интерес представляет динамическое использование ресурсов для заранее не предусмотренных транзакций управления. Эти транзакции вносят изменения в систему защиты для того, чтобы предотвратить вновь обнаруженные или прогнозируемые инциденты, сведения о которых поступили извне или были сформированы внутри самой критической инфраструктуры.

С точки зрения типологии затрат и ресурсоемкости такие изменения могут быть, по крайней мере, трех типов, условно их можно назвать: параметр, структура и сервис. Транзакции типа параметр предполагают внесение изменений в уже существующие данные – конфигурации, маршруты, размеры и т.п. Эти данные формализованы и зачастую (но не всегда!) носят количественный характер, в частности, могут определять энтропийные характеристики (длина ключа, размер и алфавит пароля и т.п.). Расход ресурсов для этого типа транзакций минимальный, но заранее он не предусматривается, поэтому эти транзакции не следует путать с регламентным управлением – формированием новых учетных записей, предоставлением ключевой информации и т.п., которое обеспечивается ресурсным бюджетом.

Более радикальным воздействием обладают транзакции типа структура, они затрагивают алгоритмические и инфраструктурные решения и, поэтому, требуют для своей реализации более ощутимых ресурсов. Эти корректировки должны привлекаться, когда возможности транзакций типа параметр исчерпываются. Например, замена алгоритма шифрования (шифратора), если действующее решение не поддерживает дальнейшее увеличение размера ключа.

Наконец, транзакции типа сервис предполагают внесение изменений в архитектуру системы защиты, в состав используемых мер и средств. Строго говоря, эти изменения выходят за рамки собственно асимптотического управления, поскольку оно выполняется на транзакционном уровне, а номенклатура мер и средств защиты – это решение операционного уровня. Но формировать и специфицировать запрос на такое изменение можно силами асимптотического управления. Масштабы этих изменений еще больше, динамика реализации ниже, поэтому ресурсные потребности могут приобретать плановый характер.

Отдельно следует рассмотреть роль модели опасностей (угроз) в части управления ресурсами при адаптивном развитии защищенности.

Представим себе некоторое множество G всех возможных опасностей, реализация которых наносит ущерб нашей критической инфраструктуре. Не будем здесь отвлекаться на проблемы рекурсивности этого универсума (скорее всего, множество G не перечислимо) и идентификации самих опасностей (множество G включает как известные, так и неизвестные опасности, на этом основано утверждение о его полноте).

На множестве 2^G подмножеств G может быть задана мера $R(g)$ остаточного риска, это совокупный риск реализации опасностей, которые не вошли в соответствующий элемент $g \in 2^G$. Для упрощения изложения будем предполагать, что вошедшие в g опасности устранены с вероятностью, равной единице, другими словами соответствующие частные риски устранены полностью. Максимум $R(g)$ достигается на пустом множестве, соответствующем отсутствию какой-либо защиты. Это риск R_0 , который оценивается при категорировании критических инфраструктур. Заметим, что хотя, строго говоря, на этапе категорирования оценивается не риск, а максимальный ущерб, этот показатель эквивалентен риску в условиях свершившегося (с вероятностью единицы) инцидента.

В результате выполнения мер по защите формируется множество g «компенсированных» опасностей и тем самым достигается соответствующий уровень остаточного риска. При этом считаем, что действует принцип монотонности для риска: добавление в g элементов («компенсированных» опасностей») в результате развития защитных мер, по крайней мере, не увеличивает остаточный риск, т.е. если $g'' \subset g'$, то $R(g'') \geq R(g')$.

Часть опасностей неизвестна, но они, тем не менее, вызывают неидентифицированные риски. Поскольку защита представляется целенаправленной деятельностью и имеет дело с установленными опасностями, каждому уровню знаний (каждому разделению множества G на известные и неизвестные опасности, т.е. каждой модели опасностей) соответствует некоторый минимальный «неидентифицированный» остаточный риск R_z , который представляет собой совокупность неидентифицированных рисков от неизвестных опасностей. «Неидентифицированный» риск не может быть снижен без развития знаний об опасностях, т.е. без расширения модели опасностей (угроз).

Формирование множества g означает реализацию некоторых мер защиты, которые будут противодействовать опасностям из этого множества, и сделают эти опасности «компенсированными». Реализация мер защиты потребует затраты определенных ресурсов. Упрощая представление об этих ресурсах, будем полагать здесь ресурсы скалярными или, по крайней мере, поддерживающими отношение порядка. Кроме того, нет оснований считать, что необходимые меры защиты могут быть реализованы единственным способом, ресурсы для формирования g могут быть использованы по-разному. Поэтому можно говорить о существовании ресурсного минимума среди возможных вариантов формирования g , и ввести на множестве 2^G меру $C(g)$ минимальных затрат для каждого $g \in 2^G$.

По аналогии с рисками будем считать действующим принцип монотонности для ресурса: добавление в g элементов («компенсированных» опасностей») в результате развития защитных мер, по крайней мере, не уменьшает минимальных затрат, т.е. если $g'' \subset g'$, то $C(g'') \leq C(g')$.

Отметим, что строго говоря, приведенные формализмы не утверждают единственности множества g , обеспечивающего конкретное значение $R(g)$, т.е. теоретически может быть несколько $g \in 2^G$, на которых достигается заданный уровень остаточного риска – это группа решений с одинаковым риском. Поэтому, говоря о множестве g , обеспечивающем уровень риска $R(g)$ следует иметь в виду представителя этой группы с минимальным значением $C(g)$.

Таким образом, каждому значению остаточного риска R между R_z и R_0 (дискретностью пренебрегаем) можно сопоставить множество (модель) «компенсированных» опасностей g и соответствующее значение минимальных затрат $C(g)$ необходимых для достижения этого уровня риска. Множество таких точек в координатах «риск-затраты» составляют область Парето, ограничивающую пространство возможных решений, все реальные решения соответствуют точкам выше этой области.

Существуют некоторые особенности управления ресурсами развития защищенности при использовании различных подходов к управлению безопасностью.

Нормативный (декларативный) подход непосредственно устанавливает номенклатуру мер защиты, в условиях фиксированного множества опасностей, которым эти меры противостоят и, следовательно, де-факто устанавливая некоторый уровень остаточного риска. Этот нормативный риск никак не исчисляется, он априорно неизвестен, но полагается допустимым.

В процессе своего формирования номенклатура мер защиты рационализируется [7]: первоначальный набор мер определяется категорией объекта [4], учитываются структурно-функциональные характеристики используемых технологий, учитываются априорные сведения об актуальности опасностей (модель угроз). Тем самым осуществляются некоторые оптимизирующие действия в отношении ресурсов, используемых для реализации мер защиты. Эти действия выполняются при первоначальном формировании номенклатуры и оперируют с относительно крупными конгломератами опасностей, соответствующих целому направлению

защиты или сервису безопасности - шифрование, управление доступом, аутентификация и т.п. Поэтому необходимый ресурс планово предоставляется фактически с избытком, независимо от реально возникающих опасностей. Тем самым при нормативном подходе всегда создается некоторый ресурсный запас, который сохраняется даже после решения оптимизационных задач.

В целом, можно утверждать, что при нормативном подходе достигаемый остаточный риск и используемый для этого ресурс - величины относительно стабильные, фактически задаваемые извне (ресурс еще можно как-то оптимизировать, управляя инфраструктурой). Поэтому изменение номенклатуры мер защиты - это планомерный процесс, обеспеченный необходимым бюджетом.

Классический рискориентированный подход отличается от нормативного тем, что остаточный риск при создании системы защиты непосредственно исчисляется и сравнивается с порогом допустимого уровня. При этом учитывается тот факт, что известные опасности «компенсируются» не полностью, и для каждой из них остается, пусть небольшая, но отличная от нуля, вероятность быть реализованной. Поэтому остаточный риск складывается из рисков неизвестных опасностей и частных остаточных рисков известных.

После достижения установленного порога, остаточный риск становится стабильным параметром, задача управления сводится к его удержанию, а внесение каких-либо изменений защищенности предполагает полный цикл управления рисками - идентификацию и анализ. Проведение таких масштабных мероприятий, несомненно, требует обеспеченности соответствующим бюджетом.

В отличие от традиционных подходов, которые не меняют структуру множества известных опасностей и не влияют на уровень минимального «неидентифицированного» риска $R_?$, асимптотическое управление каждой своей транзакцией не только уменьшает остаточный риск, но и снижает ограничение со стороны $R_?$. Это происходит в силу действия принципа монотонности риска, поскольку опасность, порождающая обрабатываемый инцидент, переводится из категории неизвестных в разряд известных.

Причем, если инцидент произошел на самом защищаемом объекте (самая критическая ситуация), это изменение требуется для предельно конкретной - «атомарной» конфигурации опасности, требующей для противодействия себе минимального расхода ресурсов. На практике могут быть внесены расширяющие обобщения, распространяющие изменения на класс однотипных инцидентов, и предполагающие увеличение используемого ресурса. Это увеличение происходит в силу действия принципа монотонности ресурса, а само обобщение делается с расчетом на противодействие будущим инцидентам, т.е. ресурс как бы запасается. Такие обобщения присутствуют и в сведениях, поступающих извне и содержащих результаты проведенного анализа инцидентов, выявленных на других критических инфраструктурах.

В заключение следует упомянуть об еще одной особенности управления ресурсами, характерной для контекста динамического развития защищенности. Это эффект т.н. высвобождаемых ресурсов. В результате объединения в процессе управления «компенсируемых» опасностей по какому-то общему признаку (тип ущерба, тактика атаки, вид уязвимости и т.п.) формируется некоторый ресурсный потенциал, и возникают дополнительные ресурсные возможности как следствие «неаддитивности» ресурса или присутствия в нем условно возобновляемой (высвобождаемой) части. Другими словами, ресурс, необходимый для защиты от совокупности двух опасностей может быть меньше, чем объединение ресурсов, необходимых для защиты от каждой из них в отдельности. Это не нарушает принцип монотонности ресурса, но означает, что в составе требуемого ресурса есть составляющая, которая при повторном востребовании может быть высвобождена. Многократное и независимое обращение за таким ресурсом приводит к накоплению высвобождаемой части, это еще один источник запаса ресурса.

Литература

1. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных структур. Научно-техническое издательство “Горячая линия - Телеком” Москва, 2021, – 239с
2. Ерохин С.Д., Петухов А.Н. Архитектура асимптотического управления безопасностью критических информационных инфраструктур //ДСПА: Вопросы применения цифровой обработки сигналов №1 2022, стр. 18-31
3. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
4. Правительство Российской Федерации. Постановление от 8 февраля 2018 г. N 127. Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической

информационной инфраструктуры российской федерации и их значений (в ред. Постановления Правительства РФ от 07.11.2025 N 1762)

5. ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования
6. Репин В. В., Елиферов В. Г. Процессный подход к управлению. Моделирование бизнес-процессов. — М.: РИА «Стандарты и качество», 2008. — 408 с. — ISBN 978-5-94938-063-5
7. Федеральная служба по техническому и экспортному контролю Российской Федерации, Приказ от 25 декабря 2017 г. N 239, Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры российской федерации (в ред. Приказа ФСТЭК России от 28 августа 2024 г. N 159)

FEATURES OF RESOURCE MANAGEMENT IN THE DEVELOPMENT OF CRITICAL INFRASTRUCTURE SECURITY

PhD Erokhin S.D.¹, PhD Petukhov A.N.², PhD Pilyugin P.L.²

¹Moscow Technical University of Communications and Informatics

²National Research University "MIET"

The resource aspects of information security management are discussed, which involve the dynamic development of protective capabilities during operation. This is relevant for critical information infrastructures, which are characterized by some a priori uncertainty of the target security parameters. Exceptional situations regarding the use of resources at certain stages of the life cycle are considered. It shows the need for multidimensional criteria for resource management and consideration of the internal structure of resources – response and functioning, as well as the relationship between the typology of costs and resource intensity with the nature of security development – parameter, structure or service. The scheme of formalization of restrictions on the level of protection and resources expended for the used hazard model is given, taking into account the "unidentified" residual risk. It is shown that asymptotic control not only increases the level of security, but also reduces the "unidentified" risk.



ЗАДАЧИ ОПТИМИЗАЦИИ РЕСУРСОВ ПРИ РАЗВИТИИ ЗАЩИЩЕННОСТИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

доц., к.т.н., Петухов А.Н., к.т.н. Пилюгин П.Л.

Национальный исследовательский университет «МИЭТ»

Обсуждаются ресурсные аспекты управления информационной безопасностью, предполагающие динамическое развитие защитных возможностей в процессе функционирования. Это актуально для критических информационных инфраструктур, которым свойственна некоторая априорная неопределенность целевых параметров защищенности. Показана эволюция структуры задач оптимизации ресурсов от самой простой, базирующейся на однократной транзакции управления, до последовательной адаптивной процедуры, ориентированной на асимптотическое динамическое развитие защищенности. Рассматриваются факторы, приводящие к кусочно-монотонному характеру развития защищенности в условиях ограниченности ресурсов и динамически меняющейся агрессивной среды. Предложена схема описания итераций процесса асимптотического управления в зависимости от иницирующих факторов для формулировки процедур управления при ограниченных ресурсах.

Характерной особенностью критических информационных инфраструктур является некоторая априорная неопределенность целевых параметров достигаемого в процессе управления уровня защищенности [1]. Это затрудняет планирование и оптимизацию ресурсов необходимых для обеспечения безопасности, особенно в условиях привлечения адаптивных методов управления информационной безопасностью, предполагающих динамическое развитие защитных возможностей непосредственно в процессе функционирования информационной системы.

Для анализа связи достигаемого уровня защищенности и необходимого для этого ресурса рассмотрим универсум G - множество всех возможных опасностей g , реализация которых наносит ущерб критической инфраструктуре. Универсум G включает как известные, так и неизвестные опасности.

Предположим, что на множестве 2^G подмножеств G задана мера $R(g)$ остаточного риска, это совокупный риск реализации опасностей, которые не вошли в соответствующее подмножество $g \subset G$, $g \in 2^G$. Максимум этой меры $R_0 = \max R(g)$ достигается на пустом множестве, соответствующем отсутствию какой-либо защиты.

Вводя в эксплуатацию средства защиты, мы формируем множество g «компенсированных» опасностей, обеспечивая некоторый уровень защищенности, достигая остаточный риск $R(g)$. При этом полагаем справедливым принцип монотонности для риска: добавление в g элементов не увеличивает соответствующий остаточный риск, т.е. если $g'' \subset g'$, то $R(g'') \geq R(g')$.

Про часть опасностей из G ничего неизвестно (либо они признаны неактуальными), но каждому представлению о «потенциале агрессии», зафиксированному в виде g , соответствует некоторый «неидентифицированный» остаточный риск R_g , который представляет собой совокупность частных неидентифицированных рисков от неизвестных опасностей. Уровень «неидентифицированного» риска априорно неизвестен, но полагается несущественным и не может быть снижен без расширения g .

Реализация мер защиты (формирование множества g) требует затраты определенных ресурсов. Будем считать эти ресурсы скалярными и поддерживающими отношение порядка. Поскольку меры защиты, обеспечивающие g , могут быть реализованы неединственным способом, соответствующие ресурсы могут быть израсходованы по-разному, и среди этих вариантов существует ресурсный минимум, позволяющий ввести на множестве 2^G меру $C(g)$ минимальных затрат для каждого $g \subset 2^G$.

Действие отношения порядка для ресурсов позволяет утверждать принцип монотонности для ресурса: добавление в g элементов не уменьшает минимальных затрат, т.е. если $g'' \subset g'$, то $C(g'') \leq C(g')$.

Можно избежать необходимости опираться на наличие конкретного знания о потенциале действующих опасностей. Для этого надо связать размер ресурса не с множеством опасностей g , а непосредственно с комплексом средств защиты Z , потребляющих этот ресурс $C(Z)$ для противодействия опасностям из g . Тогда возможен переход к аналогичной зависимости $R(Z)$ для остаточного риска при использовании комплекса средств защиты Z .

Переход к таким зависимостям упрощает постановку и решение оптимизационных задач, но при необходимости непосредственного (эксплицитного) определения остаточного риска (например, при рискориентированном подходе к управлению безопасностью) требуется отображение множества 2^G всевозможных моделей опасностей (угроз) на множество всевозможных комплексов защитных мер 2^X , где X - все доступные средства защиты. Корректная формализация такого отображения представляет собой самостоятельную проблему. Дополнительные сомнения вызывает справедливость принципа монотонности рисков по отношению к элементам множества 2^X . Кроме того, остается открытым вопрос о размерах и ограничениях «неидентифицированных» рисков.

Тем не менее, формализация процесса управления безопасностью позволяет сформулировать задачи для поиска оптимального решения для управления ресурсами.

Определим для значения остаточного риска величину R , а для его допустимого значения R_d . Пусть также для каждой совокупности используемых средств защиты Z из 2^X , определяется необходимое количество ресурсов $C(Z)$. При этом количество доступных ресурсов также ограничено величиной C_d .

В этих обозначения задачу получения оптимального управления ресурсами для обеспечения допустимого риска защиты можно сформулировать следующим образом «делаем все, что нужно, обеспечивая заданный (имплицитно) уровень риска с минимальными затратами» [1]:

$$C \rightarrow \min (C(Z) \mid Z \subset X) \text{ при } R \leq R_d \quad (1)$$

Однако в реальной практике минимизации используемых ресурсов они могут быть изначально ограничены $C(Z) \leq C_d$, и тогда при недостаточности ресурсов риск будет выше допустимого.

В рамках однократной транзакции асимптотического подхода [2] задача максимального обеспечения защиты формулируется как «делаем все, что можно, чтобы снизить риск, при ограниченных ресурсах», т.е. ограничение ресурсов учитывается явно (эксплицитно):

$$R \rightarrow \min (R(Z) \mid Z \subset X) \text{ при } C \leq C_d \quad (2)$$

Формулировку (2) можно дополнить важным ограничением из (1), так как не все значения R допустимы.

$$R \rightarrow \min (R(Z) \mid Z \subset X) \text{ при } C \leq C_d, R \leq R_d \quad (3)$$

Такое дополнение является значимым только в отношении «однопроходных» процедур оптимизации, в частности, однократной транзакции адаптивных процедур, в т.ч. асимптотического управления. Полноценная организация процесса асимптотического управления рано или поздно автоматически приведет к выполнению условия $R \leq R_d$ [3], поскольку монотонно обеспечивает рост защищенности в результате каждой транзакции управления (в этом смысл его асимптотичности). Правда, условие такого «автоматического» достижения необходимого уровня риска может не выполняться при существенной динамике потенциала действующих опасностей как в части структуры множества G , так и в части параметров соответствующих рисков. Это касается как опасностей, моделируемых в составе множества g , так и «неидентифицированных» рисков (кусочно-монотонный характер развития защищенности, рисунок 1) [4].

Из приведенных формальных постановок задачи (1), (2) и (3) следует, что все «управление» безопасностью предусматривает только один шаг, после которого либо ресурсы заканчиваются или достигается явно или неявно заданный допустимый риск. В чем же тогда состоит управление в процессе эксплуатации (развития) системы безопасности, если цель уже достигнута или оказалась недостижима на данном этапе развития в связи с тем, что ресурсы закончились? Можно сформулировать две оптимизационные задачи управления в условиях развития защищенности, связанные с наличием ресурсов или получением информации о новых ранее «неидентифицированных» рисках.

В первом случае можно использовать оставшиеся или регулярно получаемые для эксплуатации систем защиты ресурсы (эксплуатационные расходы) в соответствии с формулировкой (2) или (3).

Вторая задача управления возникает при получении новой информации об опасностях, меняющей оценку ожидаемого остаточного риска.

В общем случае предельно возможный ожидаемый риск R_0 :

$$R_0 = R + R_?$$

где R – оценка управляемых (снижаемых, ограничиваемых) рисков;

$R_?$ – неидентифицированный риск.

Можно отметить, что «неидентифицированный риск» характеризует неполноту используемой модели опасностей (угроз) – множество g . Поэтому, изменение модели опасностей (угроз) или переоценка предельно возможного ожидаемого риска могут вызывать необходимость управляющего воздействия в последовательные моменты времени t_k .

Основное условие, накладываемое в рамках асимптотического подхода к управлению безопасностью на управляющие воздействия это монотонный рост уровня защищенности после каждой транзакции управления. Пусть $R(t_k, Z_k)$ значение оценки риска в момент t_k для соответствующей этому моменту системы защитных мер Z_k :

$$R(t_{k+1}, Z_{k+1}) \leq R(t_k, Z_k), \quad (4)$$

где $\leq$ отношение частичного порядка, определенное на множестве значений функции риска..

Обращает на себя внимание отсутствие каких-либо ограничений для соотношения Z_k и Z_{k+1} , в т.ч. каких-то условий пресечения или «вложенности» одного и другого наборов средств защиты.

Управляющие воздействия инициируются как внешними и внутренними событиями. Например, в качестве таких событий могут выступать:

- различные нарушения функционирования средств обеспечения безопасности, что требует управления ими для восстановления средств защиты и поддержания требуемого уровня защищенности;
- выявление возможной уязвимости, и для ее предотвращения возможно проведение переоценки рисков и управление настройками и конфигурациями (без изменения состава) средств защиты;
- получение от внешних источников информации (например, отраслевого CERT) о неизвестной атаке или уязвимости, что может привести к переоценке рисков или изменения настройки/конфигурациями средств защиты и/или изменения их состава;
- получение общих (как правило нормативных) указаний и рекомендаций от регионального или федерального CERT и также к переоценке рисков или изменения настройки/конфигурациями средств защиты и/или изменения их состава.

Очевидно, что изменение значения функции $R(t, Z)$ в следующей точке ($t=k+1$) обусловленное обнаружением новой уязвимости (или атаки) может сделать реализуемые до этого защитные мероприятия недостаточно эффективными. Следовательно, функция $R(t, Z)$ может быть представлена как кусочно-монотонная. При этом можно отметить, что монотонные участки соответствуют принципам асимптотического управления безопасностью при наличии достаточных ресурсов.

Можно предположить, что периоды времени между моментами изменения $R(t, Z)$ могут увеличиваться в результате затруднения получения новой информации и из-за необходимости накопления необходимых ресурсов. Здесь важно учитывать дополнительное ограничение из (3).

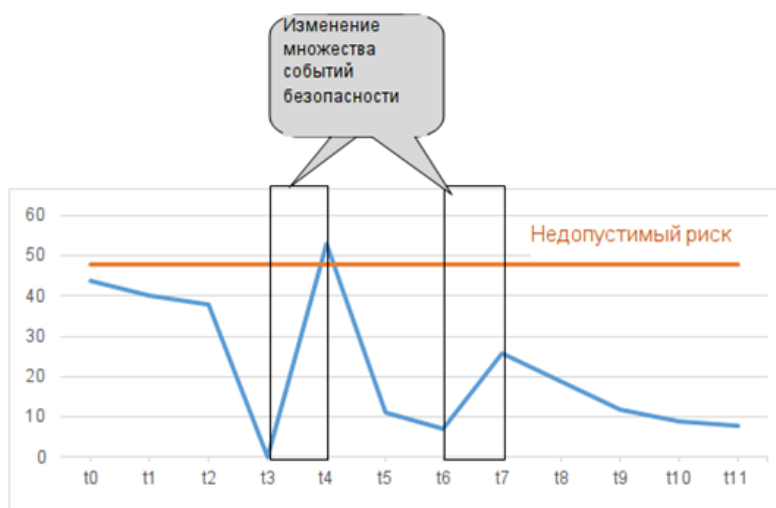


Рисунок 1. Пример кусочно-монотонной функции развития защищенности [4].

Отметим, что нарушение монотонности в оценке риска, может быть вызвано не только изменением модели опасности (угроз) множества g , но и переоценкой возможного ущерба.

Справедливо полагать, что достижение идеального состояния защищенности при асимптотическом подходе к управлению безопасностью невозможно, так как может потребовать неограниченного времени и неограниченных ресурсов, которые нужны для управляющих воздействий и ограничены доступными ресурсами.

Здесь можно выделить два типа ресурсов, которые могут и не могут использоваться для управляющих воздействий в процессе развития защищенности.

Первый вид это ресурсы, находящиеся в распоряжении оператора систем защиты объекта, например:

- Ресурсы C_3 , бюджетно выделяемые на эксплуатационные расходы, используемые в данном случае для расширения состава действующих средств защиты;
- Ресурсы C_y (вычислительные, технические, финансовые и пр.), которые могут возникнуть как следствие «неаддитивности» ресурса или присутствия в нем условно возобновляемой (высвобождаемой) части; возникают, когда ресурс, необходимый для защиты от совокупности двух опасностей может быть меньше, чем объединение ресурсов, необходимых для защиты от каждой из них в отдельности..

Второй вид ресурсов C_k это «невозвратные» ресурсы (капитальные затраты), потраченные на Z . И если использование этих Z перестало быть актуальным, а использовать их для защиты от новых опасностей невозможно, то необходимы дополнительные затраты для совершенствования системы защиты, например, при нарушении дополнительного ограничения из (3).

Таким образом, можно рассматривать доступные средства на каждом шаге управления как:

$$C_d(t) = C_3(t) + C_y(t) + C_k(t) \quad (5)$$

Очевидно, что $C_k(t)$ будет монотонно возрастать, величина $C_y(t)$ ограничена и величина этих ограничений зависит от объема и состава Z , а величины $C_3(t)$, которые условно можно считать постоянными или медленно возрастающими.

Это позволяет переформулировать постановку оптимизационной задачи (3) следующим образом:

$$R(t) \rightarrow \min (R(Z) \mid Z \subset X)$$

при

$$C(t_{k+1}) \leq C_3(t_k) + C_y(t_k) + C_k(t_k), R(t_{k+1}, Z_{k+1}) \leq R_d(t_k, Z_k) \quad (6)$$

А для монотонных участков рисунка 1 :

$$R(t) \rightarrow \min (R(Z) \mid Z \subset X)$$

при

$$R(t_{k+1}, Z_{k+1}) \leq R(t_k, Z_k), C(t_{k+1}) \leq C_3(t_k) + C_y(t_k) + C_k(t_k), R(t_{k+1}, Z_{k+1}) \leq R_d(t_k, Z_k) \quad (7)$$

Выражения (6) и (7) позволяют описать итерации процесса асимптотического управления, в зависимости от причин, инициирующих управляющее воздействие, что может быть использовано при формулировке управленческих процедур при ограничении доступных ресурсов.

Литература

1. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных структур. Научно-техническое издательство “Горячая линия - Телеком” Москва, 2021, – 239с
2. Ерохин С.Д., Петухов А.Н. Архитектура асимптотического управления безопасностью критических информационных инфраструктур //DSPA: Вопросы применения цифровой обработки сигналов №1 2022, стр. 18-31
3. Sergey Erokhin, Andrey Petukhov, Pavel Pilyugin «Adaptation processes in asymptotic safety management» IEEE Xplore 29 июня — 01 июля 2022 года «Системы синхронизации, формирования и обработки сигналов в инфокоммуникациях» СИНХРОИНФО 2022.
4. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л., Литвинюк С.П. Формальное описание асимптотического управления информационной безопасностью КИИ. Системы синхронизации, формирования и обработки сигналов, 2024, Т.15, № 6

THE TASKS OF OPTIMIZING RESOURCES WHILE DEVELOPING THE SECURITY OF CRITICAL INFRASTRUCTURES

PhD Petukhov A.N., PhD Pilyugin P.L.

National Research University "MIET"

The resource aspects of information security management are discussed, which involve the dynamic development of protective capabilities during operation. This is relevant for critical information infrastructures, which are characterized by some a priori uncertainty of the target security parameters. The evolution of the structure of resource optimization tasks from the simplest, based on a single management transaction, to a consistent adaptive procedure focused on the asymptotic dynamic development of security is shown. The factors leading to the piecewise monotonous nature of the development of security in conditions of limited resources and a dynamically changing aggressive environment are considered. A scheme is proposed to describe the iterations of the asymptotic control process depending on the initiating factors for the formulation of control procedures with limited resources.



МЕТОДЫ ОБНАРУЖЕНИЯ УТЕЧКИ ПО ТЕХНИЧЕСКОМУ КАНАЛУ, СОЗДАВАЕМОМУ ВЫСОКОЧАСТОТНЫМ ОБЛУЧЕНИЕМ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ

асс. Порхун А.С., инж. Ненашева Ю.А.

Национальный исследовательский университет «МИЭТ»

Современные системы перехвата по техническому каналу, создаваемому методом высокочастотного облучения выделенного помещения, позволяют с высоким уровнем маскировки из-за использования полуактивных закладных устройств вести перехват акустической речевой информации. Профессиональное обнаружение полуактивных закладных устройств и облучающих генераторов требует систематического сканирования радиочастот, визуального осмотра и углубленной проверки выделенного помещения на наличие электроники для точного определения местоположения закладных устройств и облучающих генераторов. В этой статье будут рассмотрены различные методы обнаружения утечки по вышеупомянутому техническому каналу и будет приведена классификация методов по различным признакам.

1) Анализ радиочастотного спектра внутри выделенного помещения.

Профессиональные радиочастотные детекторы сканируют весь спектр от 30 МГц до 12 ГГц, анализируя радиочастоты на предмет несанкционированных передач, указывающих на скрытые закладные устройства. Профессиональные детекторы имеют широкий частотный диапазон и хорошую чувствительность, могут идентифицировать слабые сигналы, передачи с переключением частот и зашифрованные сообщения [1].

1.1) Триангуляция.

Анализ спектра в реальном времени позволяет специалистам обнаружить источники сигналов методом триангуляции, различать легитимные и закладные устройства, а также обнаруживать даже сложные закладные устройства, использующие передовые методы передачи для избегания обнаружения. Триангуляция – это метод определения местоположения динамических объектов. Метод основывается на измерении углов (пеленгов), в направлении которых регистрируется максимальный уровень сигнала, в контрольных точках, их должно быть минимум две, в них устанавливаются радиопеленгаторы, разнесённые на заранее известное расстояние (англ. base). На рисунке 1 показана схема использования метода триангуляции в случае поиска источника радиоизлучений в двумерном пространстве (в одной плоскости).

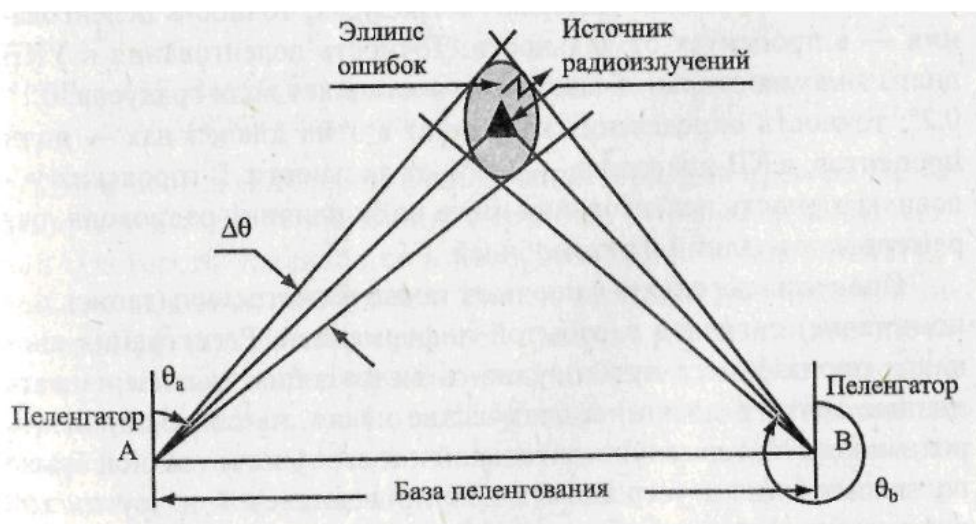


Рисунок 1 – Схема использования метода триангуляции при поиске источника радиоизлучения, $\theta_{a(b)}$ – угол между направлением на источник радиоизлучения и севером в точке пеленгатора А(В), $\Delta\theta$ – погрешность измерения угла

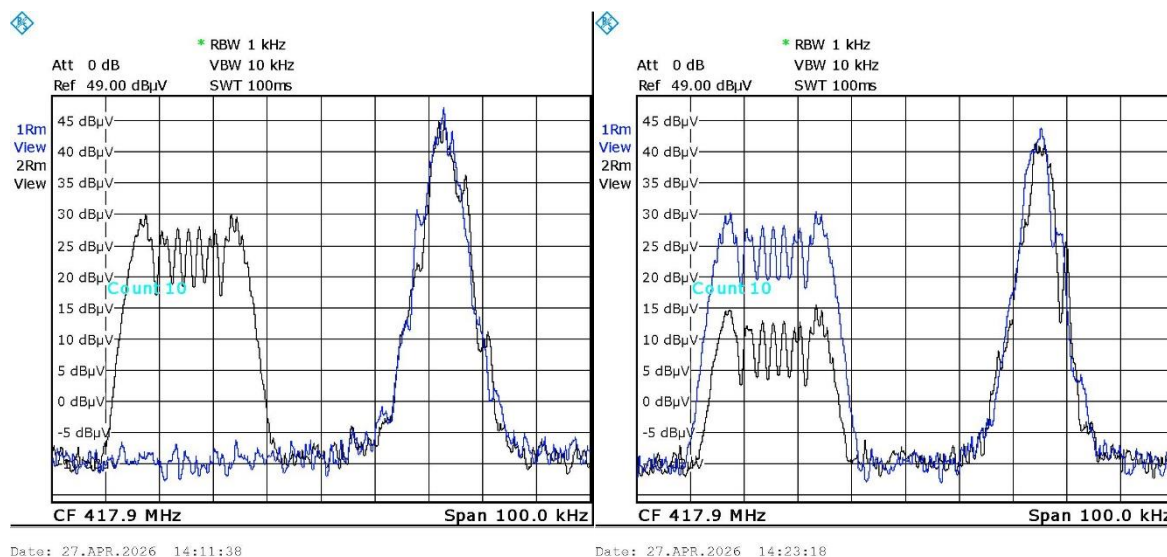
1.2) Метод опорной панорамы.

Он заключается в том, что заранее, например, в ночное время при отсутствии сигналов, связанных с закладными устройствами, в автоматическом режиме происходит измерение амплитудного спектра, то есть формируются два множества – частот и амплитуд. Затем измерение амплитудного спектра происходит в момент ведения переговоров в выделенном помещении, в этот момент работает генератор системы высокочастотного облучения и закладное устройство. После спектры сравниваются на предмет

существенной разницы в уровнях сигналов на всех диапазонах частот. Участки спектра с большой разницей в уровнях сигналов используются для передачи сигналов с закладных устройств.

1.3) Метод пространственно-разнесенного приема.

Он заключается в том, что прием сигналов ведется с двух антенн: одна находится в выделенном помещении, другая за пределами выделенного помещения, но близко к нему, например, в смежном помещении. На основе принятых сигналов строится спектр, а ввиду того, что выделенное помещение облучается направленным сигналом и закладное устройство установлено внутри выделенного помещения, спектр с антенны, которая внутри выделенного помещения, будет иметь значительно большие энергетические характеристики на определенных частотах, где работают закладки, в остальных же диапазонах разница будет несущественной. На рисунке 2 а синим цветом показана опорная панорама, черным – текущая панорама, полученная в момент передачи сигнала полуактивным закладным устройством, опорная и текущая панорамы существенно отличаются, следовательно, в диапазоне, где существенное отличие по уровню мощности, идет передача сигнала полуактивным закладным устройством. На рисунке 2 б показаны сигналы с двух антенн: синим – сигнал с первой антенны, находящейся в выделенном помещении, черным – сигнал со второй антенны, находящейся в смежном помещении, в диапазоне, где уровень мощности существенно отличается, работает полуактивное закладное устройство, находящееся в выделенном помещении, поскольку уровень сигналов от расстояния от близких источников снижается стремительно.



а)

б)

Рисунок 2 – Результаты использования методов опорной панорамы (а) и пространственно-разнесенного приема (б)

2) Нелинейная локация выделенного помещения.

Оборудование для нелинейной локации обнаруживает полупроводниковые переходы в электронных устройствах независимо от того, включено ли закладное устройство в данный момент, передает сигнал или выключено. Эта передовая технология позволяет обнаруживать скрытые закладные устройства путем идентификации электронных компонентов, содержащихся во всех современных закладных устройствах.

В отличие от радиочастотного сканирования, которое обнаруживает только активные передачи, нелинейные детекторы работают с неактивными устройствами, которые не передают сигнал в режиме реального времени [1].

Антенна нелинейного детектора облучает объект для обнаружения наличия электронных компонентов. Когда излучаемый сигнал на своем пути сталкивается с полупроводниковыми соединениями (диодами, транзисторами и т. д.), он возвращается на гармонических частотах из-за нелинейных свойств соединения.

Из-за различий вольт-амперных характеристик реальных и ложных полупроводников интенсивность отклика второй и третьей гармоник будет разной. При облучении реального полупроводника излучением отклик второй гармоники сильнее, чем третьей. Ложный полупроводник дает более сильный отклик на третьей гармонике.

3) Визуальный осмотр выделенного помещения.

Систематический визуальный осмотр включает в себя методичную проверку мест при несущественных затратах, где могут быть скрыты небольшие закладные устройства. Специалисты ищут необычные предметы, модифицированные предметы повседневного обихода или недавно установленное оборудование, в котором могут быть спрятаны скрытые закладные устройства [1]. Главные принципы проведения визуального осмотра: должен быть план осмотра, например, от центра к краям помещения, объекты не демонтируются и не разбираются, труднодоступные и скрытые области подвергаются детальному вниманию. Используемые технические средства: фонари, досмотровые зеркала и специальные эндоскопы.

4)Магнитометрия (метод индукции) выделенного помещения

Поиск металлов с помощью металлоискателя предполагает использование специализированного устройства для обнаружения скрытых металлических предметов внутри выделенного помещения (потолков, стен, ниш, полов, предметов интерьера, мебели и других различных объектов). Металлоискатели работают следующим образом: они посылают электромагнитный сигнал в определенном направлении, а затем принимают отраженный сигнал от металлических предметов [2]. Важным понятием здесь будут токи Фуко, это — токи, генерируемые переменным магнитным полем вокруг электропроводящего материала, именно эти токи генерируют свое магнитное поле, которое улавливает детектор [3].

В любом полуактивном закладном устройстве есть антенна, которая сделана из металла. Именно ее и можно обнаружить при помощи металлоискателя, несмотря на то, какие размеры и форму она имеет. Некоторые модели металлодетекторов обладают следующими особенностями.

Электромагнитные поисковые катушки. Металлодетекторы используют электромагнитные поисковые катушки для генерации магнитного поля, проникающего в глубину материалов. При взаимодействии этого поля с металлическими предметами возникает ответный сигнал, который схема детектора может распознать и использовать для точного определения местоположения объекта [2].

Идентификация цели. Современные детекторы анализируют тип металла, измеряя его проводимость и магнитные свойства. В результате этого процесса присваивается идентификатор цели, помогающий специалистам отличать важные находки, такие как полуактивные закладные устройства, от сторонних предметов, например, линий питания вспомогательных технических средств и систем [2].

Балансировка. Современные «умные» металлодетекторы адаптируются к различным условиям за счет балансировки, что снижает помехи от природных минералов. Это помогает поддерживать точность обнаружения даже в сложных условиях, таких как сильно минерализованные строительные материалы [2].

Технология Multi-IQ — это технология металлоискателя, которая одновременно посылает несколько поисковых частот. Низкие частоты лучше подходят для поиска крупных объектов на большей глубине. Высокие частоты лучше подходят для обнаружения мелких или тонких целей близко к поверхности. Используя полный диапазон частот одновременно, Multi-IQ дает вам лучшее из обоих миров. Это делает его более точным при поиске более широкого спектра целей и более надежным в сложных условиях, таких как при поиске в минерализованных материалах. Это также помогает отличить важный объект от того, который можно игнорировать. Именно поэтому он отлично подходит для всех видов поиска [2].

Технология 5Fх8 от Minelab позволяет в настройках металлоискателя выбирать одну из пяти частот: 5, 10, 15, 20 и 40 кГц. Эта универсальность, доступная в модели EQUINOX 800, позволяет пользователям регулировать частоту детектора для более эффективного обнаружения конкретных типов металлических предметов. Например, более низкие частоты, такие как 5 кГц, более эффективны для обнаружения крупных, высокопроводящих целей, таких как антенны полуактивных закладных устройств [2].

5)Рентгенография.

Для выявления скрытых полуактивных закладных устройств, предназначенных для негласного получения информации, может применяться рентгеновское излучение. Данный метод обеспечивает бесконтактную визуализацию внутренней структуры объектов, что является критически важным при работе с ценными материалами, сложными конструкциями или в условиях невозможности их демонтажа. Внешний вид оборудования и результат его работы показаны на рисунке 3.

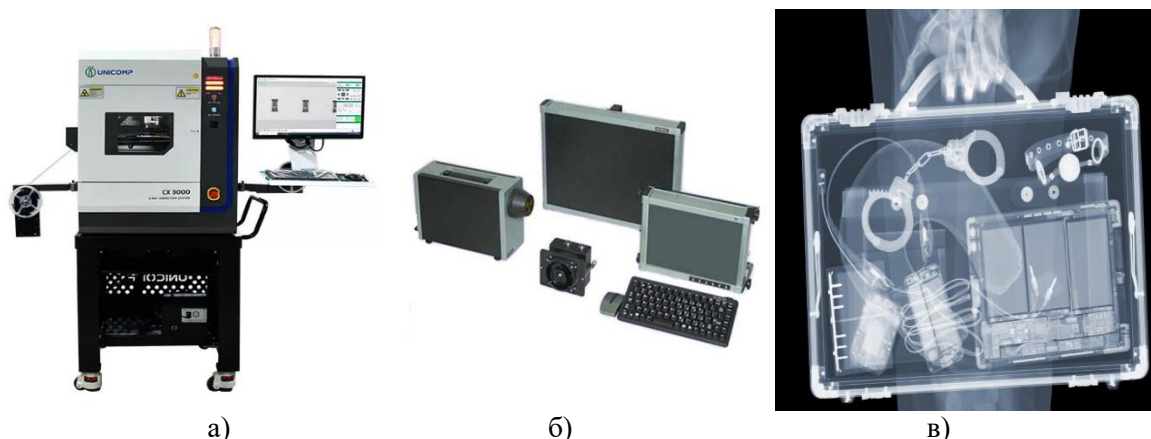


Рисунок 3 - Стационарная система рентгеновского контроля CX3000 (а), переносная досмотровая система НОРКА (б), снимок (результат работы) системы рентгеновского контроля (в)

Рентгеновское излучение - электромагнитные волны, которые состоят из фотонов. При облучении предметов волны частично проходят в глубину, которая определяется видом материалов и их плотностью. В результате таких действий образуется теневое изображение внутренней архитектуры предмета, затем оно превращается в видимое или цифровое изображение. Для поиска закладных устройств применяется «тормозное» излучение, которое получается при столкновении ускоренных электронов с различными составляющими предметов. Такое излучение содержит информацию о внутренней архитектуре предмета, что дает возможность обнаружить неестественные зоны, связанные с присутствием ЗУ.

Рентгеновская техника бывает следующих видов:

- стационарная (она нужна для анализа архитектуры больших предметов, например, железобетонных и кирпичных стен, вентиляционных шахт);
- переносная (она нужна для исследования относительно небольших предметов);
- телевизионная (дает возможность получать картинку на экране в реальном времени. Может быть использована для анализа выделенных помещений (ограждающих конструкций, предметов интерьера, офисной техники) с целью выявления закладных устройств).

Рентгеновская техника может быть использована при поиске закладных устройств в следующих местах:

- железобетонные и кирпичные стены и перекрытия;
- вентиляционные шахты и внутри потолочное пространство;
- внутренние предметы выделенного помещения (мебель, канцелярские предметы, символические драгоценные подарки, картины, электроника, печатные материалы).

Преимущества использования рентгеновского оборудования:

- анализ архитектуры предметов без их повреждения;
- высокая степень детализации (последние модели оборудования имеют разрешение до нескольких микрон, что дает возможность обнаруживать небольшие компоненты закладных устройств);
- анализ многослойных поверхностей (исследование печатных электронных плат или микросхем).

6)Тепловизионная съемка.

Обнаруживает тепловые сигнатуры от активных электронных устройств, которые могут не излучать радиосигналов, но все же генерировать обнаруживаемые тепловые излучения. Поиск закладных устройств с использованием тепловизоров базируется на регистрации тепловых изменений относительно окружения, возникающих в результате функционирования электронных схем закладных устройств. Основы технологии обнаружения состоят в том, что все закладные устройства при функционировании излучают тепло. Специальное тепловизионное оборудование имеет возможность обнаруживать незначительные колебания температуры в пространстве, что дает возможность находить активные закладные устройства исходя из их теплового излучения. В случае если закладное устройство размещено в электронном оборудовании выделенного помещения, то его поиски происходят путём обнаружения мест соединения электронных компонентов (локализованных излучающих ИК-источников) и блоков, температура внутри них отличается на большую величину от температуры внешних элементов в верхнюю сторону. Тепловизионная съемка относится к пассивным методам обнаружения закладных устройств, поскольку она не подразумевает активного воздействия на исследуемые объекты. Этот факт может быть важным при обнаружении закладных устройств, поскольку мероприятия по обнаружению происходят без лишних признаков. Тепловизионное оборудование превращает тепловое (электромагнитное) излучение в видимую человеком картинку. Оно

бывает следующих типов: портативное или специальное. Имеет следующие основные технические характеристики: разрешение и прецизионность установления температуры.

Классификация методов обнаружения утечки для рассматриваемого канала.

По обнаруживаемому объекту:

- методы обнаружения полуактивных закладных устройств (1.1, 1.2, 1.3, 2, 3, 4, 5, 6);
- методы обнаружения генераторов систем высокочастотного облучения (1.1, 1.2, 1.3).

По опасности применения:

- относительно безопасные (1.1, 1.2, 1.3, 2, 3, 4, 6); — опасные (5).

По эффективности применения:

- высокоэффективные (2, 4, 5); — низкоэффективные (1.1, 1.2, 1.3, 3, 6).

Литература

1. Comprehensive Guide to Listening Device Detection: Protect Your Privacy. — Текст : электронный // SPI Sentry Private Investigators : [сайт]. — URL: <https://www.sentryprivateinvestigators.co.uk/post/how-to-detect-listening-devices-professional-tscm-bug-sweeping-guide> (дата обращения: 24.04.2026).
2. Discover the Technology Behind Metal Detection. — Текст : электронный // MINELAB : [сайт]. — URL: <https://www.minelab.com/how-detectors-work> (дата обращения: 24.04.2026).
3. Foucault's current. — Текст : электронный // GOUDSMIT MAGNETICS : [сайт]. — URL: <https://www.goudsmitmagnetics.com/en-us/knowledge-base-foucault-current> (дата обращения: 24.04.2026).

METHODS OF LEAK DETECTION VIA A TECHNICAL CHANNEL CREATED BY HIGH-FREQUENCY IRRADIATION OF A DEDICATED ROOM

asst. Porkhun A.S., eng. Nenasheva J.A.

National Research University of Electronic Technology

Modern interception systems using a technical channel created by irradiating a designated room with high frequency allow for the interception of acoustic speech information with a high level of concealment due to the use of semi-active eavesdropping devices. Professional detection of semi-active eavesdropping devices and irradiating generators requires systematic radio frequency scanning, visual inspection, and an in-depth check of the designated room for electronics to accurately locate the eavesdropping devices and irradiating generators. This article will examine various methods for leak detection using the aforementioned technical channel and classify them based on various criteria.



РЕАЛИЗАЦИЯ ПРЕОБРАЗОВАНИЯ MIXCOLUMNS В ПОЛИНОМИАЛЬНОЙ СИСТЕМЕ КЛАССОВ ВЫЧЕТОВ

Проворнов И. А., д.т.н., проф. Калмыков И. А.

Северо-Кавказский федеральный университет

Статья посвящена повышению отказоустойчивости преобразования MixColumns, являющегося составной частью стандарта шифрования AES, за счет применения корректирующего кода, функционирующего в полиномиальной системе классов вычетов. Описываемый подход позволяет выполнять эффективное обнаружение и коррекцию всех однократных ошибок. В статье подробно описывается порядок данного корректирующего кодирования, обосновывается выбор используемых в качестве оснований такой системы полиномов, предлагаются пути дальнейших научных исследований, которые необходимы для решения задачи повышения отказоустойчивости систем шифрования на базе AES.

Введение

В настоящее время в условиях постоянного развития технологий в целом и цифровых угроз в частности, становится максимально важным обеспечение информационной безопасности критических объектов т.к. их безопасность непосредственно связана с безопасностью государства и граждан. Современные системы практически полностью основаны на информационных технологиях: без них невозможно обеспечить работу транспорта, энергетики, связи и многих других сфер промышленности.

Рост киберугроз обусловлен в т. ч. внедрением умных устройств, автоматизированных систем управления, так как это увеличивает уязвимость инфраструктуры к внешним воздействиям.

Ярким примером такой цифровизации промышленности является применение автоматизированных систем управления железнодорожным транспортом. Вместе с тем, очевидно, что негативным последствием сбоев в работе таких систем может быть возникновение аварийной ситуации. Для недопущения такого развития событий реализуется комплекс технических мер, одной из которой является применение криптографических средств защиты обрабатываемой и передаваемой информации.

Реализация преобразования MixColumns в полиномиальной системе классов вычетов

Перспективной технологией, используемой для передачи информации между элементами системы принятий решений в железнодорожной инфраструктуре, является стандарт связи LTE-R, который представляет собой специализированную мобильную связь, обеспечивающую надежную и защищенную связь между поездами, станциями, центрами управления и другими объектами. Защищенность информации в LTE-R достигается за счет реализации шифрования в соответствии с криптоалгоритмом AES, одним из этапов которого является преобразование MixColumns.

Однако, подсистема шифрования системы управления железнодорожным транспортом является одним из наиболее уязвимых к сбоям элементов, за счет наличия в её составе компонентов, чувствительных к электромагнитным помехам. Поэтому актуальным направлением совершенствования криптографических систем является разработка способов противодействия факторам, способствующим возникновению сбоев и отказов в работе рассматриваемых систем.

Из [Error! Reference source not found., Error! Reference source not found.] известно, что преобразование MixColumns представляет собой преобразование, заключающееся в умножение входного сигнала, который является матрицей размерности 1×4 , на матрицу констант размерности 4×4 . При этом элементами обеих матриц являются цифровые сигналы размерности 8 бит. Результатом такого умножения также будет являться матрица размерности 1×4 т.е. состоящая из одного столбца и четырех строк, нумерованных от 0 до 3. Тогда подобное преобразование можно представить в формульном виде согласно:

$$\begin{bmatrix} S'_{0c} \\ S'_{1c} \\ S'_{2c} \\ S'_{3c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} S_{0c} \\ S_{1c} \\ S_{2c} \\ S_{3c} \end{bmatrix}, \quad (1)$$

где $S'_{0c} - S'_{3c}$ – элементы выходного столбца;

$S_{0c} - S_{3c}$ – элементы входного столбца.

При этом согласно стандарту AES [Error! Reference source not found.], под умножением в выражении (1) понимается умножение полиномов в конечном поле Галуа (2^8) по модулю неприводимого многочлена, имеющего вид:

$$m(x) = x^8 + x^4 + x^3 + x + 1. \quad (2)$$

Такая реализация операции умножения с одной стороны позволяет обеспечить представления результата этого умножения 8 битами, что принципиально для AES, однако, с другой стороны увеличивает вычислительную сложность данного преобразования.

В свою очередь, повышение вычислительной сложности дополнительно повышает вероятность возникновения сбоев и отказов, что опять возвращает нас к необходимости разработки альтернативных способов реализации преобразования MixColumns.

В настоящее время в ряде фундаментальных работ, в т. ч. в [Error! Reference source not found., Error! Reference source not found., Error! Reference source not found., Error! Reference source not found.] доказана эффективность использования модулярной арифметики для решения задач повышения отказоустойчивости различных цифровых систем. Проведенный анализ показал, что наиболее эффективным вариантом борьбы с возникающими ошибками в ходе преобразования MixColumns будет применение корректирующего кода, описанного в [Error! Reference source not found.].

В соответствии с [Error! Reference source not found.], любое число, имеющее в полиномиальной форме вид $A = (a_1(x), a_2(x), \dots, a_k(x))$ может быть представлено в виде следующей полиномиальной системы классов вычетов (ПСКВ):

$$A = (a_1(x), a_2(x) \dots a_k(x), a_{k+1}(x), a_{k+2}(x)), \quad (3)$$

где
$$\alpha_{k+1}(x) = \sum_{i=1}^k \alpha_i(x), \quad a_{k+2}(x) = \sum_{i=1}^k i(x) \cdot a_i(x) \bmod p_{k+1}(x).$$

Такое представление чисел позволяет после их цифровой обработки (а в контексте обсуждаемой проблематики – после преобразования MixColumns) проверить наличие ошибок в выходных числах за счет последовательного выполнения операций:

- 1) Вычисление проверочных контрольных остатков:

$$a_3^*(x) = a_1(x) + a_2(x), \quad (4)$$

$$a_4^*(x) = (a_1(x) + x \cdot a_2(x)) \bmod p_3(x). \quad (5)$$

- 2) Вычисление синдромов ошибки:

$$\delta_1(x) = \alpha_3(x) + \alpha_4^*(x), \quad (6)$$

$$\delta_2(x) = \alpha_4(x) + \alpha_4^*(x). \quad (7)$$

- 3) Вычисление вектора ошибки

$$\Delta \vec{e}(x) = \begin{cases} (0, 0), & \delta_1(x) = \delta_2(x) = 0. \\ (\delta_1(x), 0), & \delta_1(x) = \delta_2(x) \neq 0. \\ f_e(\delta_1(x), \delta_2(x)), & \delta_1(x) \neq \delta_2(x). \end{cases} \quad (8)$$

- 4) Коррекция ошибки на основе значения вектора ошибки в соответствии с процедурой описанной в [Error! Reference source not found.].

Тогда для реализации вышеописанного алгоритма для процедуры MixColumns достаточно:

- 1) умножение на константы 2_{16} , 3_{16} , 1_{16} производить в табличном виде в рассматриваемой ПСКВ с основаниями:

$$\begin{aligned} p_1(x) &= x^4 + x + 1, \\ p_2(x) &= x^4 + x^3 + 1, \\ p_3(x) &= x^4 + x^3 + x^2 + 1; \end{aligned}$$

- 2) после нахождения значения каждого элемента столбца (в результате суммирования по модулю два ранее найденных остатков в ПСКВ) выполнять процедуру обнаружения ошибок в соответствии с выражениями (4)-(8);

- 3) выполнять процедуру коррекции возникших ошибок в соответствии с [Error! Reference source not found.].

Такая реализация преобразования MixColumns позволит сохранять работоспособное состояние SPN-шифратора в случае возникновения однократных ошибок и сбоев

Заключение.

Таким образом, предложенный вариант реализации преобразования MixColumns позволяет обеспечить защиту подсистемы шифрования от возникновения однократных ошибок, независимо от природы их возникновения

Перспективными направлениями данного исследования являются:

- интеграция разработанного способа в существующие SPN-системы;
- разработка элементной базы для предложенной преобразования MixColumns.

Литература

1. Прикладная криптология: методы шифрования : учебное пособие / Б. С. Ахметов, А. Г. Корченко, В. П. Сиденко и др. – Алматы : КазНУ имени К. И. Сатпаева, 2015. – 496 с.: ил.
2. Герман О. Н., Нестеренко Ю. В. Теоретико-числовые методы в криптографии: учебник для студ. учреждений высш. проф. образования //М.: Издательский центр «Академия». – 2012. – Т. 272.
3. Зензин О.С., Иванов М.А. Стандарт криптографической защиты – AES. Конечные поля / Под. ред. М.А. Иванова – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с.
4. Калмыков И.А., Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов / Под ред. Н.И. Червякова. – М.: ФИЗМАТ-ЛИТ, 2005. – 276 с.
5. Калмыков И.А., Гахов В.Р. и др. Применение корректирующих кодов полиномиальной системы классов вычетов для построения спецпроцессоров цифровой обработки сигналов / Труды международного Форума по проблемам науки, техники и образования. Том 1./ Под ред.: В.П. Савиных, В.В. Вишневого. – М.: Академия наук, 2004. – С. 133-135.
6. Червяков Н. И. и др. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях //Москва: ФИЗМАТЛИТ. – 2017.
7. Инютин С. А. Вычислительные задачи большой алгоритмической сложности и модулярная арифметика //Вестник Тюменского государственного университета.– 2002. № 3.
8. Гончаров П. С., Калмыков М. И., Степанова Е. П. Непозиционный код класса вычетов в параллельных технологиях цифровой обработки сигналов //Успехи современного естествознания. – 2014. – №. 3. – С. 102-107.
9. Калмыков И. А. и др. Алгоритм коррекции ошибок в модулярном коде классов вычетов, обеспечивающий повышение отказоустойчивости систем OFDM //Инженерный вестник Дона. – 2024. – №. 2 (110). – С. 20.

IMPLEMENTATION OF THE MIXCOLUMNS TRANSFORMATION IN A POLYNOMIAL SYSTEM OF RESIDUE CLASSES

Provornov I.A., Kalmykov I.A.

North-Caucasus Federal University

This article explores improving the fault tolerance of the MixColumns transform, an integral part of the AES encryption standard, by using a correction year operating within a polynomial system of residue classes. The described approach enables efficient detection and correction of all single-error errors. The article describes in detail the procedure for this correction coding, justifies the choice of polynomials used as bases for this system, and proposes avenues for further research needed to improve the fault tolerance of AES-based encryption systems.



СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ БИБЛИОТЕК ПОЛНОСТЬЮ ГОМОМОРФНОГО ШИФРОВАНИЯ

асп. Синицын А.А.¹, проф. Бабенко М.Г.²

¹ Институт системного программирования им. В.П. Иванникова Российской академии наук

² Северо-Кавказский федеральный университет

Представлен сравнительный анализ библиотек полностью гомоморфного шифрования. Рассмотрена эволюция ГШ от теоретической разработки Gentry (2009) до современных практических реализаций. Проанализированы технические характеристики схем. 10 библиотек были сравнены по следующим критериям: поддерживаемые схемы, типы бутстреппинга, алгоритмы переключения ключей, производительность и потребление памяти. Приведены результаты тестов из открытых источников. Даны рекомендации по выбору библиотеки в зависимости от задачи.

Введение

Полностью гомоморфное шифрование (ПГШ) – это класс алгоритмов в криптографии, позволяющий обрабатывать зашифрованные данные без их раскрытия. Идея была сформулирована в 1978 году: Ривест, Адлеман и Дертхоуц описали концепцию. Но полноценная реализация появилась только в 2009-м, благодаря диссертации Крейга Джентри [1].

GUI актуально для конфиденциальных облачных вычислений. Машинного обучения. Защиты персональных данных. Apple уже интегрировала FHE в iOS 18 для идентификации звонящих в реальном времени [2]. Microsoft применяет её в SEAL-PIR и APSI. Поэтому цель доклада - систематизировать современные библиотеки FHE, проанализировав их технические характеристики и производительность.

1. Классификация схем полностью гомоморфного шифрования

Схемы BGV (Brakerski-Gentry-Vaikuntanathan, 2011) и BFV (Brakerski/Fan-Vercauteren, 2012) реализуют точную арифметику в конечных полях. Основное различие - в управлении шумом: BGV использует modulus switching после каждого умножения, BFV - масштабирование при декодировании. BGV быстрее при больших модулях открытого текста, BFV при малых [3]. Обе схемы допускают реализацию в Системе Остаточных Классов (СОК), позволяющем избежать арифметики больших чисел.

Схема CKKS (Cheon-Kim-Kim-Song, 2016) поддерживает приближённую арифметику над вещественными числами с фиксированной точкой. Ключевая операция – это перемасштабирование: после умножения масштаб шифротекста возводится в квадрат, операция перемасштабирования делит шифротекст на масштабирующий фактор, отбрасывая модуль и контролируя рост шума. CKKS оптимальна для машинного обучения и обработки сигналов.

Схемы TFHE и APHE реализуют пошаговое бутстрапирование (англ. gate-by-gate bootstrapping) для булевых схем. В отличие от BGV/BFV/CKKS, где бутстреппинг выполняется редко, в TFHE обновляется шифротекст после каждой операции за 6–13 мс [4]. Программируемый бутстреппинг (англ. Programmable Bootstrapping (PBS)) позволяет одновременно с обновлением шума вычислять произвольную таблицу истинности (англ. Look-Up Table).

2. Сравнительный анализ библиотек

Для сравнения библиотек использовались следующие критерии: (1) поддерживаемые схемы и их полнота реализации. (2) наличие и тип бутстреппинга. (3) алгоритмы переключения ключей. (4) производительность базовых операций в мс. (5) потребление памяти при фиксированной глубине вычислений; (6) особенности.

В таблице 1 представлены технические характеристики 10 библиотек ПГШ.

Таблица 1

Технические характеристики библиотек ПГШ.

Библиотека	Язык	Схемы	Bootstrap	Key Switch	Особенности
OpenFHE 1.5	C++	BGV, BFV, CKKS, TFHE, FHEW	Все	BV, GHS, Hybrid	Scheme switching
SEAL 4.3	C++	BFV, CKKS	Нет	BV, GHS	Простота API
HElib	C++	BGV, CKKS	BGV	GHS	Ciphertext packing
TFHE-rs 1.5	Rust	TFHE	PBS	Да	Целые 8-256 бит
Lattigo 6.1	Go	BGV, BFV, CKKS, RGSW	CKKS	Да	Multiparty, WASM
Concrete 2.10	Python	TFHE	PBS	Да	FHE-компилятор
HEaAN 4.0	C++	CKKS	Да	Да	4-е пок. CKKS
Apple Swift	Swift	BFV	Нет	Да	iOS 18, PIR
HEIR	MLIR	Все*	*	—	88 проходов опт.
Phantom	CUDA	BFV, CKKS	Нет	Да	GPU-ускорение

Библиотека OpenFHE (версия 1.5.1) с открытым исходным кодом — наиболее функционально полная открытая реализация ПГШ; объединила специалистов проектов PALISADE, HElib и HEAAN. Поддерживает все основные схемы (BFV, BGV, CKKS, FHEW, CGGI). Отличительная возможность – переключение между схемами CKKS и FHEW: в рамках единого вычисления возможно перейти из CKKS в FHEW-подобную схему, выполнить неарифметическую операцию (сравнение, выделение знака, функцию активации) посредством программируемого бутстреппинга и вернуть результат в CKKS. Для переключения ключа реализованы три алгоритма — BV (поразрядное разложение без вспомогательных модулей; высокий рост шума), GHS (расширение модуля простым множителем; минимальный шум ценой увеличения размерности кольца) и гибридный, сочетающий оба подхода и принятый по умолчанию.

Библиотека Microsoft SEAL (последняя версия 4.3) не поддерживает бутстреппинг, что ограничивает доступную мультипликативную глубину вычислений заранее заданной величиной. Иными словами, реализует исключительно ПГШ с ограниченным количеством уровней операций. Данная библиотека имеет высокое качество документации и развитую экосистему сопутствующих инструментов. Компилятор EVA автоматически расставляет операции перемасштабирования и релинеаризации при генерации программ для схемы CKKS. Библиотека SEAL-PIR реализует конфиденциальное извлечение информации из БД. Инструмент APSI – позволяет выполнять конфиденциальное вычисление пересечения множеств. Для ускорения теоретико-числового преобразования (ТЧП) применяется библиотека Intel HEXL, использующая векторные инструкции AVX-512.

Библиотека HElib одна из первых широко используемых реализаций ПГШ, разрабатываемая исследовательской группой IBM (Ш. Халеви, В. Шуп). Написана на C++17 и опирается на библиотеку теории чисел NTL для арифметики больших чисел; реализует схемы BGV с поддержкой бутстреппинга и CKKS. Отличительная особенность — глубоко проработанные методы плотной упаковки шифротекстов по Смарту–Веркаутеру, обеспечивающие эффективное выполнение SIMD-операций над зашифрованными векторами, а также набор оптимизаций Джентри–Халеви–Смарты; реализованы автоматическое управление шумом и многопоточное исполнение. HElib послужила референсной реализацией для пакета IBM HElayers и оказала существенное влияние на архитектуру последующих библиотек, в частности OpenFHE. Распространяется по открытой лицензии Apache 2.0.

Библиотека TFHE-rs (последняя версия 1.5) компании Zama является эталонной реализацией схемы TFHE на языке Rust. Время выполнения программируемого бутстреппинга на одном ядре процессора Intel i9-9900K составляет 13 мс; оптимизация с использованием блочно-двоичных ключей сокращает это значение до 6,4 мс при сохранении того же уровня криптографической стойкости [4]. Библиотека поддерживает гомоморфную арифметику над зашифрованными целыми числами разрядностью 8, 16, 32, 64, 128 и 256 бит. Совместно с TFHE-rs развивается компилятор Concrete (текущая версия 2.10), транслирующий программы на подмножестве языка Python с синтаксисом, аналогичным библиотеке NumPy, в вызовы низкоуровневых функций TFHE-rs.

Библиотека Lattigo (последняя версия 6.1.1) - единственная реализация полностью гомоморфного шифрования промышленного уровня на языке Go. Поддерживается пакетный бутстреппинг схемы CKKS: при размерности кольца 32 768 он выполняется за 18 с с точностью 19,1 бит [5]. Реализованы протоколы многостороннего гомоморфного шифрования с пороговым дешифрованием, а также возможность компиляции в WebAssembly для исполнения в браузерах. Среди существующих библиотек Lattigo демонстрирует наиболее быструю генерацию ключей: на одноплатном компьютере Raspberry Pi 4 она опережает альтернативные реализации в 12,7 раза [6].

Компилятор Concrete (текущая версия 2.10, компания Zama) транслирует программы на подмножестве языка Python с синтаксисом, аналогичным библиотеке NumPy, в вызовы низкоуровневых функций TFHE-gs. Основная задача - снизить порог входа для разработчиков, не обладающих криптографической подготовкой: компилятор автоматически подбирает параметры схемы, расставляет операции бутстреппинга и переключения ключей, выполняет квантование вычислений. Сопутствующий пакет Concrete ML обеспечивает обучение и применение базовых моделей машинного обучения (линейная регрессия, деревья решений, неглубокие нейронные сети) на зашифрованных данных без необходимости работы с криптографическими примитивами напрямую.

Библиотека HEaaN компании CryptoLab - коммерческая реализация полностью гомоморфного шифрования четвёртого поколения, в основу которой положена схема CKKS. Разрабатывается группой Чхона (Cheon) в Сеульском национальном университете и компанией-спин-офф CryptoLab; в последних версиях помимо CKKS поддерживается также BFV. Отличительные особенности - собственные реализации сравнения и сортировки над зашифрованными вещественными числами, традиционно считавшиеся узким местом схем приближённой арифметики, а также аппаратное ускорение на графических процессорах. По сообщениям разработчиков, HEaaN опережает открытые библиотеки на задачах нейросетевого вывода в среднем в десятки раз; библиотека интегрирована в IBM HELayers - программный комплекс анализа на зашифрованных данных. Распространяется по коммерческой лицензии, что отличает её от прочих рассмотренных в работе библиотек.

Пакет swift-homomorphic-encryption компании Apple, опубликованный в августе 2024 г., представляет собой реализацию полностью гомоморфного шифрования на языке Swift. Поддерживается схема BFV с параметрами 128-битной постквантовой стойкости. На основе библиотеки построено приложение конфиденциального извлечения информации из базы данных (PIR), которое в системе iOS 18 используется для функции Live Caller ID Lookup — определения сведений о входящем телефонном номере без раскрытия номера серверу. По состоянию на 2026 г. это, по-видимому, наиболее массовое промышленное развёртывание ПГШ: технология применяется на сотнях миллионов устройств. Пакет распространяется по открытой лицензии Apache 2.0.

HEIR (Homomorphic Encryption Intermediate Representation) - открытый компиляторный инструментарий для ПГШ, разрабатываемый компанией Google. В отличие от рассмотренных выше библиотек, HEIR не реализует криптографические схемы непосредственно, а представляет собой набор диалектов на базе среды MLIR (Multi-Level Intermediate Representation), описывающих гомоморфные вычисления на различных уровнях абстракции - от схемо-независимого представления программы до низкоуровневых операций над полиномами в системе остаточных классов. Поддерживается компиляция с входных языков Python и PyTorch, генерация кода под несколько целевых библиотек (в качестве основной используется OpenFHE), а также под аппаратные ускорители. Цель проекта — обеспечить переносимость гомоморфных вычислений между схемами, библиотеками и оборудованием, а также служить единой платформой для исследовательских оптимизаций.

PhantomFHE - открытая библиотека ПГШ с ускорением на графических процессорах NVIDIA, реализованная на CUDA/C++ с привязками для языка Python. Поддерживаются схемы BGV, BFV и CKKS; бутстреппинг в текущей версии не реализован. Авторы - исследовательская группа из Нанкинского университета аэронавтики и космонавтики, Фуданьского университета и лаборатории Чжэцзян - предлагают усовершенствованную реализацию гибридного переключения ключей и стратегии слияния вычислительных ядер CUDA, существенно сокращающие задержку и расход памяти на графическом процессоре. По данным авторов, PhantomFHE даёт ускорение в десятки - сотни раз относительно реализаций на центральном процессоре. Распространяется по лицензии GPLv3 и ориентирована преимущественно на задачи частного машинного обучения с высокими требованиями к пропускной способности.

4. Анализ производительности

В таблице 2 приведены результаты бенчмарков из открытых источников [4, 5, 6, 7]

Таблица 2.

Производительность операций FHE

Операция	Библиотека	Время	Условия
TFHE gate bootstrap	TFHE	13 мс	i9-9900k, 1 ядро
TFHE gate bootstrap	TFHE (block keys)	6.4 мс	Оптимизация [4]
BGV сложение	HElib	0.021 мс	N=32768
BGV сложение	SEAL	0.04 мс	N=32768
BGV сложение	Lattigo	0.059 мс	N=32768

CKKS bootstrap	Lattigo	18 с	N=32768, 19.1 бит
300 FHE сложений	OpenFHE	4 с	Linux
300 FHE сложений	SEAL	7 с	Linux

Потребление памяти библиотеками существенно различается: при мультипликативной глубине вычислений в 20 уровней OpenFHE расходует 400 МБ оперативной памяти под Linux, тогда как SEAL - более 1200 МБ [7]. Размер ключа бутстреппинга в схеме TFHE составляет 109 МБ при стандартной конфигурации и 60 МБ при использовании блочно-двоичных ключей, что соответствует сокращению на 45 % [4]. При равном уровне стойкости OpenFHE расходует менее половины оперативной памяти, требуемой SEAL. На репрезентативной задаче из 300 последовательных гомоморфных сложений OpenFHE опережает SEAL почти в два раза при равных параметрах [7].

Заключение

В работе проведён сравнительный анализ десяти современных библиотек ПГШ. Сопоставление показало, что ни одна из реализаций не доминирует по всему набору критериев: OpenFHE объединяет все основные схемы и поддерживает переключение между ними, HEaaN и HELib специализируются на CKKS/BGV, TFHE-rg и Concrete на булевых схемах. Разрыв производительности между схемами достигает нескольких порядков: программируемый бутстреппинг TFHE 6–13 мс на одну операцию, бутстреппинг CKKS даже в оптимизированной Lattigo около 18 с. Расход памяти при равной стойкости различается в разы (400 МБ у OpenFHE против свыше 1200 МБ у SEAL при глубине 20 уровней). В экосистеме отчётливо проявляется смещение от криптографических библиотек к компиляторным инструментам (HEIR, Concrete, EVA), а развёртывание ПГШ в iOS 18 фиксирует переход технологии в стадию массового применения. Основным открытым вопросом остаётся стоимость бутстреппинга для всех схем кроме TFHE; её снижение составляет ключевое направление дальнейших оптимизаций, в том числе с использованием продвинутых представлений в системе остаточных классов. **Благодарности.** Исследование выполнено за счет гранта Российского научного фонда №25-71-30007, <https://rscf.ru/project/25-71-30007/>.

Литература

1. Gentry, C. A Fully Homomorphic Encryption Scheme: PhD thesis / C. Gentry. – Stanford University, 2009.–209p.
2. Combining Machine Learning and Homomorphic Encryption in the Apple Ecosystem [Электронный ресурс] // Apple ML Research. – 2024. – Режим доступа: <https://machinelearning.apple.com/research/homomorphic-encryption> (дата обращения: 10.05.2026).
3. Kim, A. Revisiting Homomorphic Encryption Schemes for Finite Fields / A. Kim [et al.] // Cryptology ePrint Archive. – 2021. – Report 2021/204.
4. Lee, C. Faster TFHE Bootstrapping with Block Binary Keys / C. Lee, S. Min, J. Seo, Y. Song // ASIA CCS '23: Proc. 2023 ACM Asia Conf. on Computer and Communications Security. — ACM, 2023. — P. 879–893. (Cryptology ePrint Archive, Report 2023/958).
5. Mouchet, C. Lattigo: a Multiparty Homomorphic Encryption Library in Go / C. Mouchet [et al.] // WAHC 2020. – P. 64–70.
6. Benchmarking FHE Libraries in IoT Devices // Proc. 11th Int. Conf. NSS. – ACM, 2024. – doi:10.1145/3704522.3704546.
7. Badawi, A. Cross-Platform Benchmarking of SEAL and OpenFHE / A. Badawi [et al.] // Cryptology ePrint Archive. – 2025. – Report 2025/473.

COMPARATIVE ANALYSIS OF MODERN FULLY HOMOMORPHIC ENCRYPTION LIBRARIES

PhD stud. A.A. Sinitsyn¹, prof. M.G. Babenko²

¹ Ivannikov Institute for System Programming of the Russian Academy of Sciences (ISP RAS), Moscow

² North Caucasus Federal University, Stavropol

. A comparative analysis of fully homomorphic encryption libraries is presented. The evolution of homomorphic encryption from Gentry's theoretical construction (2009) to modern practical implementations is reviewed. Technical characteristics of the schemes are analyzed. Ten libraries are compared by the following criteria: supported schemes,

bootstrapping types, key switching algorithms, performance, and memory consumption. Benchmark results from open sources are presented. Recommendations for library selection depending on the task are provided.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НАПРАВЛЕННОГО МИКРОФОНА С ФАЗИРОВАННОЙ МИКРОФОННОЙ РЕШЕТКОЙ

д.т.н. доц. Щербаков В.А., студ. Смирнов А.С.

Национальный исследовательский университет «МИЭТ»

В работе решается задача исследования пространственной избирательности средств перехвата акустической информации на основе микрофонных фазированных решеток. Предложена математическая модель такой решетки, реализованная в среде конечно-элементного моделирования COMSOL Multiphysics с применением алгоритма Delay-and-Sum. Проведены вычислительные эксперименты, направленные на исследование влияния количества элементов, шага решетки и частоты сигнала на диаграмму направленности. Показано, что модель адекватно отражает теоретические закономерности и может быть использована для оценки характеристик перспективных средств перехвата акустической информации, а также в учебном процессе.

Совершенствование технических средств разведки, в частности прямого акустического канала утечки информации, требует разработки адекватных методов и моделей для оценки потенциальных возможностей устройств перехвата речевой (акустической информации). Традиционные ненаправленные микрофоны обладают низкой пространственной избирательностью, что существенно ограничивает их применение в условиях естественных шумов и при необходимости выделения сигнала от удаленного источника. Одним из наиболее перспективных направлений является создание микрофонных фазированных решеток (МФР), позволяющих формировать узкую диаграмму направленности (ДН) с электронным управлением без механического перемещения конструкции.

Однако проектирование таких устройств сопряжено с необходимостью решения сложной обратной задачи: требуется достоверно оценить, как изменение конструктивных параметров (количество микрофонов, шаг между ними, рабочая частота) влияют на реальную пространственную избирательность микрофонной системы. Существующие аналитические модели, основанные на теории антенных решеток, дают лишь приближенные оценки и не учитывают явления, связанные с распространением звуковых волн в конкретной акустической среде (отражения, дифракцию, поглощение). Более того, в доступной литературе отсутствует универсальная модель и методический аппарат, позволяющая на этапе проектирования достоверно провести моделирование и исследование характеристик МФР с целью оптимизации её параметров без дорогостоящих натурных испытаний. В связи с этим целью данной работы является анализ возможности создания математической модели микрофонной фазированной решетки в среде конечно-элементного моделирования COMSOL Multiphysics с реализацией алгоритма Delay-and-Sum, а также исследование влияния геометрических параметров (числа элементов и шага) и частоты сигнала на диаграмму направленности такой решетки.

Диаграмма направленности любой антенной решетки (в том числе акустической) представляет собой зависимость уровня принимаемого сигнала от угла прихода волны. Для линейной эквидистантной решетки из N ненаправленных элементов с шагом l , на которую падает плоская волна с частотой f (скорость звука c), комплексная диаграмма направленности по мощности описывается известным выражением, связывающим ширину главного лепестка с апертурой решетки (произведением $N \cdot l$) и длиной волны $\lambda = c/f$. Теоретически установлено, что увеличение количества элементов или их шага сужает главный лепесток, однако превышение шагом половины длины волны приводит к появлению дополнительных (решетчатых) лепестков, что ухудшает однозначность пеленгования источника акустического сигнала [1]. Для линейной эквидистантной решетки из N ненаправленных элементов с шагом l , на которую падает плоская волна с частотой f (скорость звука c), комплексная ДН $D(\theta)$ по мощности описывается следующей формулой:

$$D(\theta) = \left| \frac{\sin(N \cdot \frac{\pi f l}{c} \cdot \sin \theta)}{N \sin(\frac{\pi f l}{c} \cdot \sin \theta)} \right|^2, \quad (1)$$

где θ – направление прихода волн.

Для формирования управляемого луча в данной работе использован алгоритм Delay-and-Sum (задержка и суммирование). Суть его заключается в компенсации временных задержек сигнала τ_i на каждом микрофоне в зависимости от заданного угла наведения и последующем когерентном сложении обработанных сигналов x_i . Математически выходной сигнал решетки $Y(t)$ для направления θ_0 описывается следующей формулой [2]:

$$Y(t) = \sum x_i \cdot (t - \tau_i), \text{ где } \tau_i = \frac{(i-1) \cdot l \cdot \sin(\theta)}{c}, \quad (2)$$

где l – шаг решетки.

Таким образом, изменяя набор задержек, можно сканировать пространство без физического поворота конструкции.

В качестве инструмента для моделирования была выбрана среда COMSOL Multiphysics (акустический модуль), реализующая метод конечных элементов. Данный выбор обусловлен следующими преимуществами: возможность создания двумерных и трехмерных геометрических примитивов с произвольными граничными условиями, учет отражений и дифракции, высокая точность расчета акустического давления в заданных точках (условных микрофонах). Моделируемое пространство включает прямоугольную область, заполненную воздухом, содержащую линейную решетку из N точечных приемников, расположенных вдоль оси X с заданным шагом, обеспечивающую формирование плоской волны сигнала, приходящей с различных углов (от -90° до $+90^\circ$) (рисунок 1).

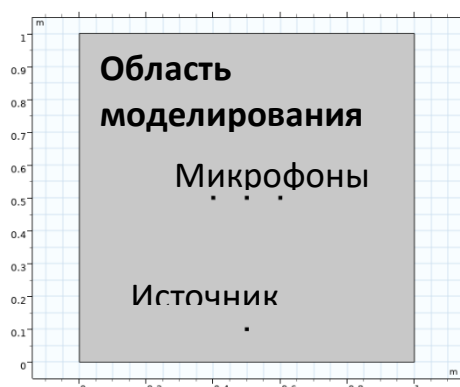


Рисунок 1 – Моделируемое пространство в среде моделирования в COMSOL

Чтобы приходящий фронт волны был плоским при использовании одиночного источника сигнала источник должен располагаться в дальней зоне микрофонной решетки.

Для получения диаграммы направленности решетки при фиксированном угле наведения (в экспериментах выбирался угол 30°) был реализован следующий алгоритм. На первом шаге строилась конечно-элементная модель среды с заданными параметрами (воздух, поглощающие границы для исключения лишних отражений). Затем для каждого угла прихода θ с шагом в 1° проводились измерения комплексной амплитуды акустического давления в точках, соответствующих положению микрофонов (рисунок 2).

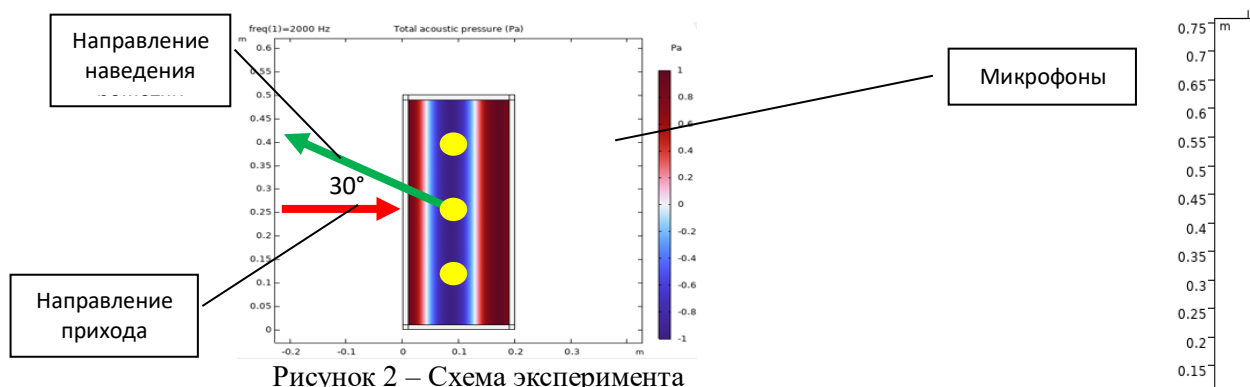


Рисунок 2 – Схема эксперимента

Далее, в соответствии с алгоритмом Delay-and-Sum, для каждого элемента решетки вычислялась требуемая временная задержка, необходимая для компенсации разности хода волны при наведении на угол 30° . Сигналы сдвигались и суммировались когерентно, после чего амплитуда полученного суммарного сигнала переводилась в децибелы относительно максимума.

Построение диаграммы направленности производилось в полярных и декартовых координатах. Параметры решетки варьировались в широких пределах: число элементов выбиралось от 2 до 8, шаг от 5 см до 30 см, частота сигнала 1000 и 2000 Гц.

При фиксированном малом шаге ($l = 17,15$ м, что значительно меньше половины длины волны $\lambda \approx 34$ см) были получены диаграммы направленности для $N = 2$ и $N = 8$. Увеличение числа элементов привело к заметному сужению главного лепестка: его ширина по уровню -3 дБ уменьшилась примерно с 60° до 15°

(рисунок 3). Одновременно вырос коэффициент направленного действия (КНД). Этот результат полностью согласуется с теорией, согласно которой разрешающая способность решетки пропорциональна её суммарной апертуре $N \cdot l$ [3], что в свою очередь характеризует достоверность проведенного моделирования.

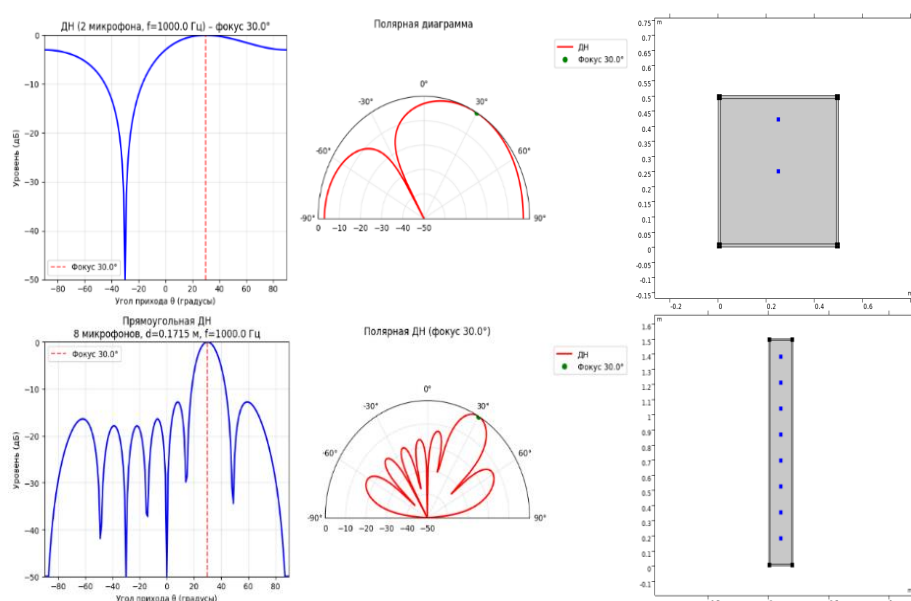


Рисунок 3 – Результаты моделирования для $N = 2$ и $N = 8$ при $l = 17,15$ см

Для решетки из пяти элементов ($N = 5$) сравнивались ДН при шаге 5 см и 30 см. При увеличении шага главный лепесток сузился, однако, при $l = 30$ см (что составляет примерно $0,43\lambda$ на частоте 1000 Гц) на диаграмме появились дополнительные максимумы (лепестки) на углах около $\pm 50^\circ$ (рисунок 4).

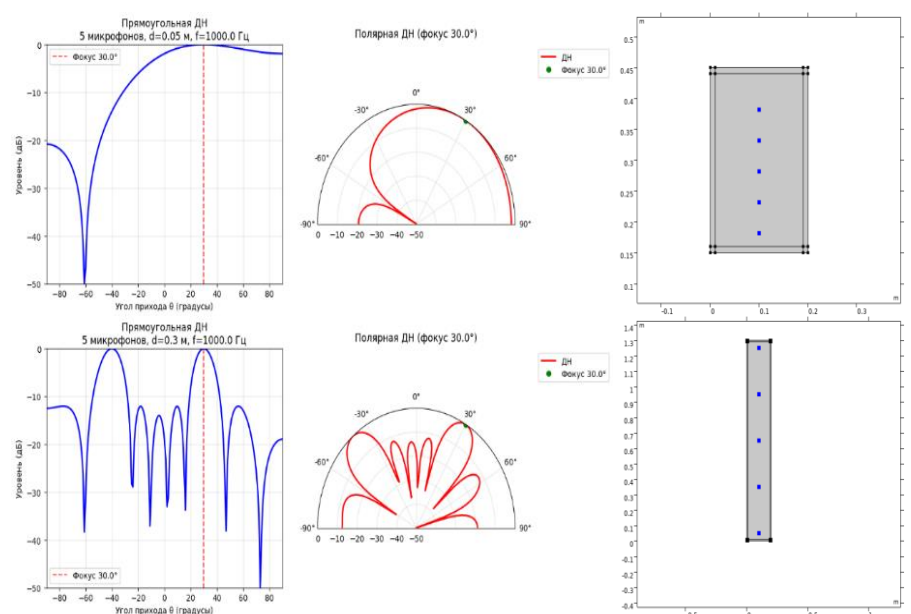


Рисунок 4 – Результаты моделирования для $l = 5$ см и $l = 30$ см при $N = 5$

Дальнейшее увеличение шага до 8–16 см приводило к тому, что эти боковые лепестки становились соизмеримыми с главным, что делает невозможным однозначное пеленгование источника. Таким образом, эксперимент подтверждает классический критерий, согласно которому шаг решетки не должен превышать половины длины волны рабочей частоты [4].

При неизменных $N = 5$ и $l = 0,1$ см были получены ДН для частот 1000 Гц и 2000 Гц. Увеличение частоты вдвое привело к сужению главного лепестка также примерно вдвое, что объясняется уменьшением длины волны и, как следствие, увеличением электрической длины решетки в волновых размерах. Кроме того, на частоте 2000 Гц шаг решетки (0,1 см) стал составлять уже около $0,6\lambda$, из-за чего на ДН появились небольшие боковые лепестки (рисунок 5).

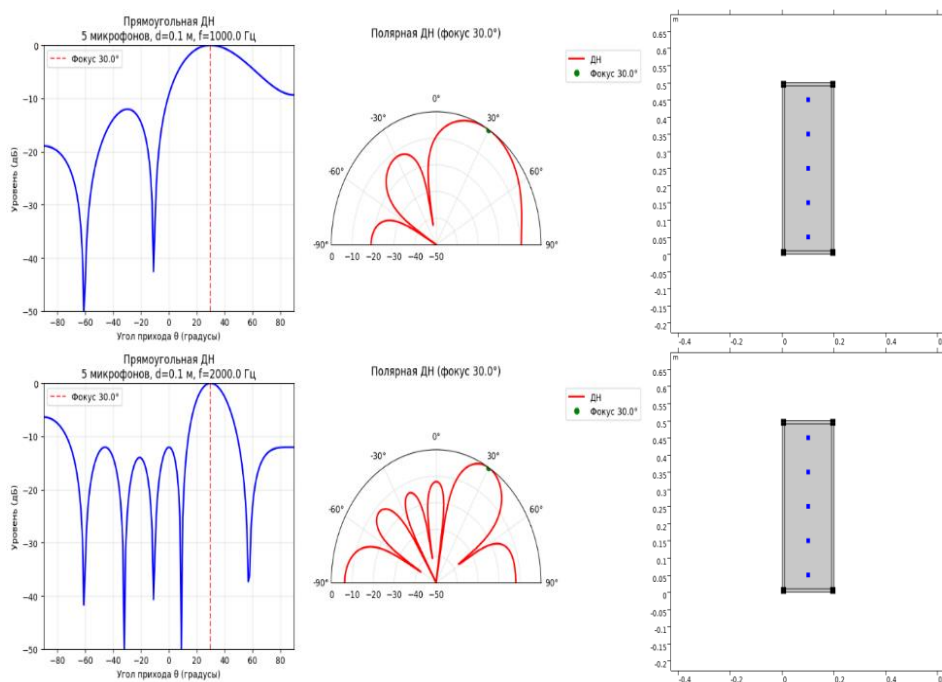


Рисунок 5 – Результаты моделирования для $f = 1000$ Гц и $f = 2000$ Гц при $N = 5$, $l = 0,1$ см

Для проверки адекватности разработанной модели проведено сравнение полученных в среде COMSOL диаграмм направленности с теоретическими кривыми, рассчитанными по формуле для линейной решетки. Для конфигураций с числом элементов $N \leq 8$ и шагом $l \leq \lambda/4$ расхождение по ширине главного лепестка не превысило 5%, а по уровню боковых лепестков – 2 дБ.

Небольшие отклонения объясняются дискретизацией конечно-элементной сетки. В целом, модель корректно воспроизводит основные физические эффекты, такие как: сужение луча при росте N и l , появление решетчатых лепестков при $l > \lambda/2$, частотную зависимость разрешающей способности.

Это позволяет использовать её для обоснованного выбора параметров МФР на этапе проектирования, а также в учебном процессе для демонстрации работы фазированных микрофонных решеток.

В ходе выполненной работы подтверждена возможность проектирования микрофонной фазированной решетки в среде COMSOL Multiphysics с реализацией алгоритма Delay-and-Sum и исследования её характеристик.

Полученные диаграммы направленности МФР для широкого диапазона параметров (число элементов от 2 до 8, шаг от 5 до 30 см, частоты 1000 и 2000 Гц) качественно и количественно соответствуют теоретическим закономерностям. Экспериментально установлено, что увеличение количества микрофонов и шага решетки сужает главный лепесток, но при $l > \lambda/2$ возникают боковые лепестки, снижающие пространственную избирательность, а повышение частоты аналогично увеличению электрических размеров микрофонной решетки. Разработанная модель может служить инструментом для обоснованного выбора параметров систем перехвата речевого (акустического) сигнала с требуемой направленностью, а также использоваться в учебных курсах по технической защите информации.

Литература

1. Смирнов А.С. Разработка математической модели направленного микрофона с фазированной микрофонной решеткой // Тезисы докладов 33-й Всероссийской межвузовской научно-технической конференции «Микроэлектроника и информатика-2026». – М.: МИЭТ, 2026.

2. Greensted A. Delay Sum Beamforming // The Lab Book Pages. — 2012. — URL: <http://www.labbookpages.co.uk/audio/beamforming/delaySum.html> (дата обращения: 01.04.2026).
3. Silverman H. F., Patterson W. R., Sachar J. Factors affecting the performance of large-aperture microphone arrays // The Journal of the Acoustical Society of America. — 2002. — Vol. 111, iss. 5. — P. 2140–2157. — DOI: 10.1121/1.1471895.
4. Jia Y. Far-field MEMS microphone array beamforming – Measurements, simulations, and design. — Master of Applied Science Thesis. — Burnaby, Canada: Simon Fraser University, 2020. — 95 p.

MATHEMATICAL MODEL OF A DIRECTIONAL MICROPHONE WITH A PHASED ARRAY MICROPHONE

Dr. Sci., Prof. Shcherbakov V.A., stud. Smirnov S.A.

National Research University of Electronic Technology

The paper addresses the problem of studying the spatial selectivity of acoustic information interception devices based on microphone phased arrays. A mathematical model of such an array has been proposed and implemented in the COMSOL Multiphysics finite element modeling environment using the Delay-and-Sum algorithm. Computational experiments have been conducted to investigate the impact of the number of elements, the array spacing, and the signal frequency on the radiation pattern. It has been shown that the model accurately reflects theoretical principles and can be used to evaluate the performance of advanced acoustic information interception devices, as well as in the educational process.



ДЕТЕРМИНИРОВАННЫЕ МОДЕЛИ ОЦЕНКИ РИСКОВ РЕАЛИЗАЦИИ КИБЕРУГРОЗ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ

асп. Татарчук М.Д., студ. Кочедыков С.С., студ. Ерасов А.Б.

Национальный исследовательский университет «МИЭТ»

В статье приведены описание и результаты применения комплекса из четырёх детерминированных моделей для автоматизированной оценки рисков киберугроз в критической информационной инфраструктуре (КИИ). Разработанный комплекс включает модели построения сценариев атак, статической оценки вероятности их реализации, визуализации результатов и формирования ранжированного плана внедрения контрмер. Исходными данными являются перечень активов КИИ, топология сети, база техник атак (в том числе в области состязательного машинного обучения), перечень контрмер и оценки их эффективности. Расчёты проводились в два этапа. На первом этапе осуществлялось построение всех возможных сценариев атак и расчёт их вероятностей. На втором этапе производилось ранжирование контрмер по весу (сумме вероятностей сценариев, в которых контрмера применима) и визуализация наиболее вероятных сценариев. Анализ полученных результатов показал, что при сумме эффективностей контрмер, равной или превышающей 1, вероятность реализации угрозы обнуляется; при отсутствии контрмер вероятность достигает 1. Ранжирование контрмер позволяет выделить наиболее критичные средства защиты. Разработанные модели подтверждают принципиальную возможность автоматизации этапов оценки рисков, однако функционируют на уровне статических алгоритмов без элементов самообучения.

Одним из наиболее актуальных направлений в области информационной безопасности критической информационной инфраструктуры является разработка методов автоматизированной оценки рисков реализации киберугроз [1, 2]. Классические подходы к управлению рисками оперируют статическими формулами и субъективными экспертными оценками, что недостаточно для современных условий [3]. Для автоматизации оценки рисков предлагается использование комплекса детерминированных моделей, работающих на основе перебора, построения графов и математических вычислений [4].

Целью данной работы является описание комплекса из четырёх детерминированных моделей (построение сценариев атак, оценка вероятности, визуализация, формирование плана обработки) и демонстрация его работы на тестовых данных в предметной области состязательного машинного обучения (AML) [5, 6].

На рисунке 1 представлена архитектура обработки данных комплекса детерминированных моделей оценки рисков.



Рисунок 1 – Архитектура обработки данных комплекса детерминированных моделей оценки рисков

Модель 1. Построение сценариев атак. С использованием перечня активов КИИ (включая их тип, сетевые требования и права доступа), топологии сети и базы знаний техник атак модель в автоматическом режиме выстраивает возможную последовательность действий нарушителя.

Модель 2. Оценка вероятности сценариев. Модель статически оценивает вероятность реализации каждого сценария с учётом действующих контрмер и их эффективности. Входные данные: сценарии атак,

база контрмер с привязкой к техникам, оценки эффективности E (0 — полная защита, 0,5 — частичная, 1 — отсутствие защиты).

Модель 3. Визуализация сценариев. Модель обеспечивает графическое представление наиболее вероятных сценариев с цветовым кодированием техник по степени риска.

Модель 4. Формирование плана обработки сценариев. Модель формирует ранжированный перечень контрмер на основе веса — суммы вероятностей всех сценариев, в которых контрмера применима.

Расчёты проводились в два этапа.

На первом этапе формировались исходные данные и производился расчёт вероятностей сценариев. В качестве предметной области использованы техники состязательного машинного обучения (AML), описывающие атаки на системы искусственного интеллекта [7, 8].

Исходные данные для модели 2 (оценка вероятности сценариев) представлены в таблице 1.

Таблица 1

Исходные данные для модели (фрагмент)

№ сценария	Техника атаки (AML)	Контрмера	Эффективность E
1	Отравление обучающих данных	Верификация входных данных	0,7
1	Отравление обучающих данных	Мониторинг дрейфа концепций	0,3
2	Уклонение (Evasion)	Защита от обратного проектирования	0,5
2	Уклонение (Evasion)	Обнаружение аномалий	0,4
3	Инференс-атака	Ограничение числа запросов	0,2
4	Компрометация конвейера ML	Контроль целостности данных	0

Расчёт вероятности для каждого сценария выполнялся по формуле

$$P = \min(1, 1 - \sum_{i=1}^n E_i), \quad (1)$$

где E_i — эффективность i -й контрмеры ($0 \leq E_i \leq 1$).

Результаты расчёта вероятности сценариев приведены в таблице 2.

Таблица 2

Результаты расчёта вероятности сценариев

№ сценария	Сумма E	Вероятность P
1	1,0	0
2	0,9	0,1
3	0,2	0,8
4	0	1,0

На втором этапе производилось ранжирование контрмер и визуализация результатов. Вес контрмеры рассчитывался как сумма вероятностей всех сценариев, в которых она может быть применена. Контрмеры ранжировались по убыванию веса.

Результаты ранжирования контрмер представлены в таблице 3.

Таблица 3

Ранжирование контрмер

Контрмера	Вес (сумма вероятностей сценариев)	Приоритет
Контроль целостности данных	1,0 (сценарий 4) + 0,1 (сценарий 2) = 1,1	1
Верификация входных данных	0,1 (сценарий 2) + 0,8 (сценарий 3) = 0,9	2
Ограничение числа запросов	0,8 (сценарий 3)	3

Мониторинг дрейфа концепций	0,1 (сценарий 2)	4
Защита от обратного проектирования	0,1 (сценарий 2)	4
Обнаружение аномалий	0,1 (сценарий 2)	4

Анализ данных, представленных в таблицах 2 и 3, позволяет сделать следующие выводы.

При сумме эффективностей контрмер, равной или превышающей 1 (сценарий 1), итоговая вероятность реализации угрозы обнуляется. Это соответствует логике работы модели 2: если совокупность применённых контрмер полностью перекрывает возможность реализации техники атаки, то угроза считается нейтрализованной. При отсутствии реализации каких-либо контрмер (сценарий 4) вероятность достигает 1, что означает безусловную реализуемость атаки при наличии соответствующей уязвимости.

Ранжирование контрмер показало, что контрмерой с наибольшим приоритетом является «контроль целостности данных», которая имеет вес 1,1. Данный показатель свидетельствует о применимости этой контрмеры к сценариям 2 и 4, совокупная вероятность которых является наибольшей

Ограничения предметной области.

Существенным ограничением разработанного комплекса является его фокусировка на техниках состязательного машинного обучения (AML). В используемую базу входят атаки типа отравления обучающих выборок, уклонения, инференс-атаки и компрометации конвейеров машинного обучения. Соответственно, контрмеры нацелены на защиту ИИ-компонентов: верификацию входных данных, предотвращение обратного проектирования моделей, мониторинг дрейфа концепций.

Вместе с тем спектр реальных угроз для КИИ существенно шире. Он охватывает воздействие на промышленные протоколы (Modbus, IEC 61850, DNP3), компрометацию программируемых логических контроллеров, нарушение физических процессов через сегмент операционных технологий, а также атаки на смежные сегменты информационной инфраструктуры. Разработанные модели не покрывают указанные типы угроз, что делает необходимым расширение базы техник и контрмер.

Представленный комплекс детерминированных моделей обеспечивает автоматизацию этапов построения сценариев атак, статической оценки вероятности, визуализации и ранжирования контрмер. Вместе с тем модели функционируют на уровне статических алгоритмов, не обладая элементами самообучения и адаптации. Они не способны отслеживать изменения в поведении злоумышленника, появление новых эксплойтов или модификацию конфигурации защищаемой системы без повторного пересмотра исходных данных. Данный уровень автоматизации соответствует базовому. Полученные результаты могут служить основой для последующего внедрения динамических механизмов.

Практические рекомендации.

На основе проведённого анализа можно сформулировать следующие рекомендации.

- 1) при ранжировании контрмер необходимо использовать комбинированный критерий, учитывающий, как вес (сумму вероятностей сценариев), так и максимальную вероятность среди сценариев, в которых контрмера применима;
- 2) расширение базы техник атак должно охватывать не только AML-угрозы, но и весь спектр угроз, характерных для КИИ (угрозы промышленных протоколов, программно-контролируемых контроллеров);
- 3) для перехода к полноценному адаптивному управлению необходимо внедрение динамических механизмов и обратной связи.

Литература

1. Qi J., Wang J. Bridging Artificial Intelligence and Railway Cybersecurity: A Comprehensive Anomaly Detection Review // Transportation Research Record: Journal of the Transportation Research Board. – 2025. – Vol. 2679, No. 5. – P. 232-255. – DOI: 10.1177/03611981241302335.
2. Лецкий Э.К., Гуров А.И. Интегрирование искусственного интеллекта в функциональное тестирование критической информационной инфраструктуры железнодорожного транспорта // Интеллектуальные технологии на транспорте. – 2025. – №1 (41). – С. 14-19. – DOI: 10.20295/2413-2527-2025-141-14-19

3. Рытов М.Ю., Мусиенко Н.О., Громов Ю.Ю. Подход к определению актуальных негативных последствий при реализации угроз информационной безопасности // Промышленные АСУ и контроллеры. – 2021. – №9. – С. 41-50. – DOI: 10.25791/asu.9.2021.1311.
4. Markin P.V., Dushkin A.V., Kochedykov S.S. Express assessment method for the risk of impaired functional stability information and communication system in conditions cyber attacks // Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus 2019), Saint Petersburg — Moscow, 28-30 января 2019 года. – Saint Petersburg — Moscow: Institute of Electrical and Electronics Engineers Inc., 2019. – P. 1754-1757. – DOI: 10.1109/ElConRus.2019.8657323.
5. Кочедыков С.С. Инфраструктурный конфликт программного обеспечения критической информационной инфраструктуры в условиях деструктивных воздействий кибератак // Computational Nanotechnology. – 2025. – Т.12, №4. – С. 143-154. – DOI: 10.33693/2313-223X-2025-12-4-143-154. – EDN: HJYCWE.
6. Здольник В.В., Минин Ю.В., Кочедыков С.С., Душкин А.В., Новосельцев В.И. Математические модели киберугроз на программное обеспечение автоматизированной системы управления // Промышленные АСУ и контроллеры. – 2018. – №2. – С. 43-55.
7. Громов Ю.Ю., Карасев П.И., Коршунов Д.С., Ершов Н.С. Аудит информационной безопасности АСУ // Промышленные АСУ и контроллеры. – 2023. – №3. – С. 30-36. – DOI: 10.25791/asu.3.2023.1424.
8. Новосельцев В.И., Елисеев А.И., Кочедыков С.С., Душкин А.В. Математическая модель процесса обработки и защиты информации в автоматизированных системах управления критически важными объектами // Промышленные АСУ и контроллеры. – 2017. – №9. – С. 33-46.

DETERMINISTIC MODELS FOR ASSESSING THE RISKS OF CYBER THREATS TO CRITICAL INFORMATION INFRASTRUCTURE

postgr. Tatarchuk M.D., stud. Kochedykov S.S., stud. Erasov A.B.

National Research University of Electronic Technology

This article describes and applies the results of a suite of four deterministic models for automated cyberthreat risk assessment in critical information infrastructure (CII). The developed suite includes models for constructing attack scenarios, statically assessing the probability of their implementation, visualizing the results, and generating a ranked countermeasure implementation plan. The initial data includes a list of CII assets, network topology, a database of attack techniques (including those in the field of adversarial machine learning), a list of countermeasures, and an assessment of their effectiveness. The calculations were conducted in two stages. The first stage involved constructing all possible attack scenarios and calculating their probabilities. The second stage involved ranking the countermeasures by weight (the sum of the probabilities of scenarios in which the countermeasure is applicable) and visualizing the most likely scenarios. Analysis of the obtained results showed that when the sum of the countermeasure effectiveness is equal to or greater than 1, the probability of a threat being realized is zero; in the absence of countermeasures, the probability reaches 1. Ranking the countermeasures allows us to identify the most critical security measures. The developed models confirm the fundamental possibility of automating risk assessment stages; however, they function at the level of static algorithms without self-learning elements.



ДЕЦЕНТРАЛИЗОВАННАЯ МОДЕЛЬ ЦИФРОВОЙ ИДЕНТИЧНОСТИ ПОЛЬЗОВАТЕЛЕЙ ВЕБ-СЕРВИСОВ

студ. Томчук Д.Э.¹, доц., к.ф.-м.н Бутакова Н.Г.^{1,2}

¹Национальный исследовательский университет «МИЭТ»

²Московский политехнический университет

Предлагается децентрализованная модель цифровой идентичности пользователей веб-сервисов, обеспечивающая подтверждение пользовательских атрибутов без необходимости централизованного хранения персональных данных. Модель основана на использовании криптографически подтверждаемых атрибутов и протоколов доказательства знания, позволяющих проверять выполнение заданных условий для атрибутов без раскрытия их фактических значений. В случаях, когда веб-сервису требуется получение полного значения атрибута, предусмотрен механизм передачи данных с криптографическим подтверждением их подлинности и фиксацией операций обработки в распределённом реестре. Использование блокчейн-инфраструктуры обеспечивает неизменяемую историю выдачи и отзыва согласия на обработку данных и позволяет осуществлять последующий аудит операций. Разработана экспериментальная программная реализация, демонстрирующая работу модели цифровой идентичности.

Развитие цифровых сервисов привело к росту числа систем, требующих идентификации пользователей, при этом цифровая идентичность в большинстве случаев реализуется в виде централизованных профилей с персональными данными. Концентрация таких данных в инфраструктуре сервисов повышает риски их компрометации и приводит к передаче избыточной информации при подтверждении пользовательских свойств.

В качестве альтернативы централизованным системам рассматривается модель цифровой идентичности, в которой пользователь самостоятельно управляет своими атрибутами. В такой модели атрибуты могут быть выданы доверенными организациями, подтверждающими их достоверность. В качестве подобных издателей могут выступать государственные информационные системы, например портал Государственных услуг (Госуслуги), обладающий проверенной информацией о пользователях. При взаимодействии пользователя с веб-сервисом возможны два типа требований к атрибутам: проверка выполнения условия без раскрытия значения и получение полного значения атрибута. В соответствии с этим в модели предусмотрены два режима – селективного раскрытия, при котором передаётся только факт выполнения условия, и полного раскрытия, необходимого для выполнения отдельных операций.

К атрибутам, используемым в режиме селективного раскрытия, могут относиться достижение пользователем установленного возрастного порога (например, старше 18 лет), наличие регистрации в определённом регионе, наличие гражданства конкретного государства, принадлежность пользователя к определённой организации или образовательному учреждению, а также наличие подтверждённого банковского счёта или статуса налогоплательщика. В этих случаях веб-сервис получает лишь подтверждение выполнения заданного условия для атрибута, тогда как его фактическое значение не передаётся системе.

Во режиме полного открытия значения атрибута пользователь предоставляет веб-сервису фактическое значение атрибута, если это необходимо для выполнения операции. К таким случаям могут относиться регистрация в финансовых сервисах с передачей даты рождения и паспортных данных, подтверждение личности в государственных системах, указание адреса для доставки, предоставление банковских реквизитов. В этих ситуациях атрибут передаётся вместе с цифровой подписью доверенной организации, что позволяет проверить его подлинность, а факт передачи может фиксироваться в распределённом реестре, формируя неизменяемую историю обработки данных.

В рамках рассматриваемой модели цифровая идентичность представляется как множество атрибутов:

$$ID_u = \{A_1, A_2, \dots, A_n\},$$

где ID_u – цифровая идентичность пользователя u ,

A_i – i -ый атрибут цифровой идентичности,

n – количество атрибутов.

Каждый атрибут включает имя атрибута, его значение и цифровую подпись, сформированную доверенной организацией:

$$A_i = (name_i, v_i, \delta_i), \quad (1)$$

где $name_i$ – имя атрибута,

v_i – значение атрибута,

δ_i – значение цифровой подписи издателя атрибута.

Цифровая подпись позволяет обеспечить проверяемость атрибутов независимо от источника их хранения [1]. При этом каждый атрибут может быть использован отдельно от других, что даёт возможность подтверждать только те свойства пользователя, которые необходимы для выполнения конкретной операции.

Такая организация позволяет избежать передачи избыточной информации при взаимодействии с веб-сервисами.

Формирование цифровой идентичности пользователя начинается с генерации криптографического идентификатора, который используется для связывания атрибутов идентичности с их владельцем. Такой идентификатор формируется на основе асимметричной криптографической системы и представляет собой пару ключей: секретного и публичного. Секретный ключ хранится только у пользователя и используется для выполнения операций, связанных с управлением цифровой идентичностью, тогда как публичный ключ может быть передан другим участникам системы и используется как открытый идентификатор пользователя.

Процедура генерации ключевой пары начинается с выбора пользователем случайного секретного значения из множества целых чисел [3]:

$$sk_u \in Z_p,$$

где sk_u – секретный ключ пользователя u ,

Z_p – множество из p целых чисел $\{0, 1, \dots, p - 1\}$.

После этого вычисляется соответствующий публичный ключ:

$$pk_u = g^{sk_u},$$

где pk_u – публичный ключ пользователя u ,

g – генератор циклической мультипликативной группы по модулю p .

Полученный публичный ключ используется как уникальный идентификатор пользователя в системе. Благодаря этому атрибуты цифровой идентичности могут быть криптографически связаны с конкретным субъектом и использоваться при взаимодействии с различными сервисами без необходимости повторной регистрации пользователя в каждой системе.

Процесс получения атрибута начинается с проверки сведений, предоставленных пользователем. После подтверждения достоверности информации издатель формирует криптографически удостоверенный атрибут. Для этого создаётся сообщение, содержащее имя атрибута, его значение и идентификатор пользователя [2]:

$$m_i = H(name_i \parallel v_i \parallel pk_u), \quad (2)$$

где $H()$ – хэш-функция.

Далее выполняется процедура формирования цифровой подписи [3]. Вычисляется параметр:

$$R = g^k$$

После этого вычисляется значение:

$$e = H(R \parallel m_i) \quad (3)$$

Затем формируется параметр подписи:

$$s = k + e \cdot sk_I,$$

где sk_I – секретный ключ издателя атрибута.

В конечном счете, цифровая подпись имеет вид:

$$\delta_i = (R, s)$$

Полученная подпись включается в структуру атрибута, формируя криптографически подтверждённую запись. Наличие цифровой подписи позволяет проверять подлинность атрибутов и гарантирует, что они были выданы доверенной организацией и не подвергались изменению.

При взаимодействии пользователя с веб-сервисом возникает необходимость подтверждения достоверности атрибутов цифровой идентичности. В ряде практических сценариев веб-сервису требуется лишь подтверждение выполнения определённого условия для атрибута пользователя. Например, при проверке возраста достаточно удостовериться, что пользователь достиг установленного возрастного порога (18 лет), без передачи точной даты рождения.

В режиме селективного раскрытия атрибутов перед выполнением процедуры доказательства веб-сервис должен убедиться, что используемый атрибут был выдан доверенной организацией и не подвергался изменению. Для этого выполняется проверка цифровой подписи издателя атрибута. На первом этапе сервис восстанавливает сообщение, использованное при формировании атрибута – формула (2). После этого вычисляется хэш-значение, необходимое для проверки подписи – формула (3). Затем выполняется проверка равенства, связывающего параметры подписи, публичный ключ издателя и вычисленное значение хэш-:

$$g^s = R \cdot pk_I^e \quad (4)$$

Если данное равенство выполняется, веб-сервис делает вывод о корректности подписи и достоверности атрибута.

После подтверждения подлинности атрибута пользователь может доказать выполнение требуемого условия для его значения без раскрытия самого значения. Для реализации такого механизма используется криптографический протокол доказательства с нулевым разглашением.

На первом этапе пользователь формирует коммитмент, представляющий собой криптографическое значение, которое скрывает исходное значение атрибута, но фиксирует его математически:

$$C = g^v \cdot h^r,$$

где h – генератор циклической мультипликативной группы по модулю p ,
 r – случайное число.

Коммитмент вычисляется на основе значения атрибута и случайного числа, что исключает возможность восстановления исходного значения без знания соответствующих параметров. Благодаря этому веб-сервис не получает доступа к значению атрибута, но может проверить корректность доказательства.

После формирования коммитмента пользователь создаёт доказательство знания значения, скрытого внутри него. Для этого выбираются случайные параметры:

$$r_v, r_r \in Z_p$$

И вычисляется вспомогательное значение, используемое в процессе доказательства:

$$T = g^{r_v} \cdot h^{r_r}$$

Формируется криптографический вызов, вычисляемый с использованием хэш-функции:

$$c = H(C \parallel T)$$

На основе полученного вызова пользователь формирует ответы протокола, которые включают параметры, связанные со значением атрибута и случайными величинами:

$$s_v = r_v + c \cdot v,$$

$$s_r = r_r + c \cdot r$$

Итоговое доказательство представляет собой набор параметров, передаваемых веб-сервису для проверки корректности вычислений:

$$\pi = (C, T, s_v, s_r)$$

Получив доказательство, веб-сервис выполняет процедуру проверки. Для этого сначала вычисляется значение криптографического вызова, аналогичное использованному пользователем:

$$c = H(C \parallel T)$$

Затем проверяется выполнение равенства, связывающего параметры доказательства, коммитмент и вспомогательное значение:

$$g^{s_v} \cdot h^{s_r} = T \cdot C^c$$

Если равенство выполняется, сервис делает вывод о том, что пользователь действительно обладает соответствующим атрибутом и что доказательство сформировано корректно. При этом значение атрибута остаётся скрытым и не передаётся сервису.

Если требуется предоставить атрибут в полном виде, например, при регистрации в финансовых сервисах, оформлении государственных услуг или выполнении юридически значимых действий, пользователь предоставляет атрибут вместе с его криптографическим подтверждением, выданным доверенной организацией (1), что позволяет веб-сервису проверить подлинность и корректность полученных данных.

После получения атрибута веб-сервис выполняет проверку его подлинности как в случае с селективным раскрытием и затем на основе полученного сообщения проверяется цифровая подпись издателя атрибута – формулы (3),(4).

Если проверка выполняется успешно, веб-сервис делает вывод о том, что атрибут был выдан доверенной организацией и не подвергался изменению. После этого значение атрибута может быть использовано для выполнения требуемой операции в системе.

Перед передачей атрибута пользователь предоставляет согласие на его использование веб-сервисом. Факт такого согласия может фиксироваться в распределённом реестре. При этом в реестре не сохраняется само значение атрибута, поскольку это противоречило бы требованиям конфиденциальности персональных данных. Вместо этого фиксируется его криптографическое представление в виде хэш-значения [2].

После этого в распределённый реестр добавляется запись, содержащая информацию о выполненной операции обработки атрибута:

$$E = (pk_u, pk_s, H(A_i), op, t),$$

где E – запись в распределённом реестре,

pk_s – публичный ключ веб-сервиса, кому предоставлен доступ,

op – тип операции,

t – временная метка операции.

Тип операции op может принимать различные значения. Например, операция выдачи атрибута доверенной организацией, предоставление пользователем согласия на использование атрибута веб-сервисом или отзыв ранее предоставленного согласия.

Поскольку записи в распределённом реестре являются неизменяемыми, отзыв ранее предоставленного доступа реализуется добавлением новой записи с типом операции отзыва. В этом случае последняя запись

для соответствующего атрибута и веб-сервиса указывает на прекращение действия ранее выданного разрешения. После фиксации операции отзыва веб-сервис получает уведомление о прекращении действия согласия пользователя, что означает невозможность дальнейшей обработки соответствующих персональных данных.

Неизменяемость записей распределённого реестра позволяет обеспечить возможность последующего аудита операций обработки данных. При необходимости любой участник системы может проверить факт выдачи согласия, определить веб-сервис, которому был предоставлен доступ к атрибуту, а также установить момент времени выдачи и отзыва такого согласия. В случае нарушения правил обработки персональных данных записи распределённого реестра могут служить криптографически подтверждаемым доказательством факта и времени выполнения соответствующих операций.

Для проведения численного эксперимента была разработана программа на языке Python с графическим интерфейсом.

На рисунке 1 представлен результат работы централизованной модели, в которой пользователь передаёт персональные данные веб-сервису для проверки атрибута (в примере - возраста). При этом в обоих случаях – как при проверке условия, так и при необходимости получения полного значения – данные передаются в открытом виде, обрабатываются и сохраняются в системе.

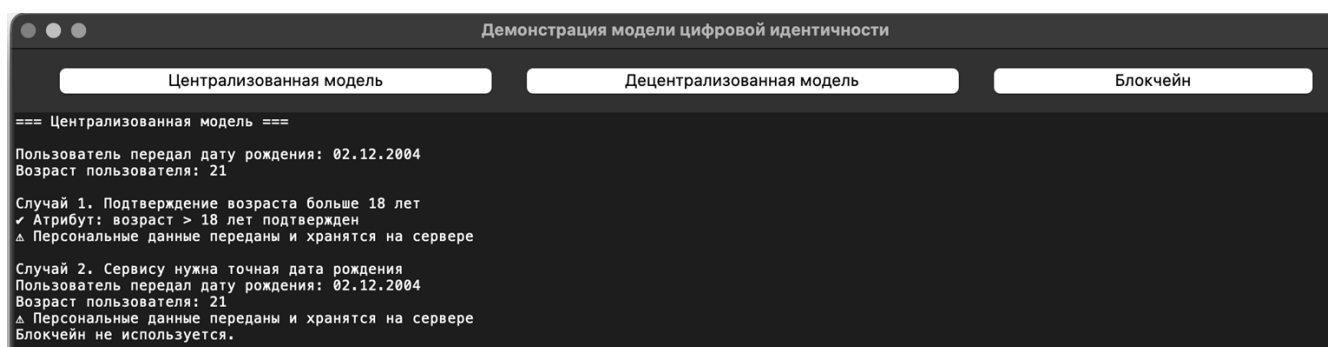


Рисунок 1. Демонстрация работы централизованной модели

На рисунке 2 представлен результат работы децентрализованной модели, также включающий два сценария. В первом случае используется криптографическое доказательство знания, позволяющее подтвердить выполнение условия без раскрытия значения атрибута – персональные данные не передаются и не сохраняются. Во втором случае пользователь предоставляет атрибут в полном виде с криптографическим подтверждением, а факт выдачи и последующего отзыва согласия фиксируется в распределённом реестре, формируя проверяемую историю обработки данных.

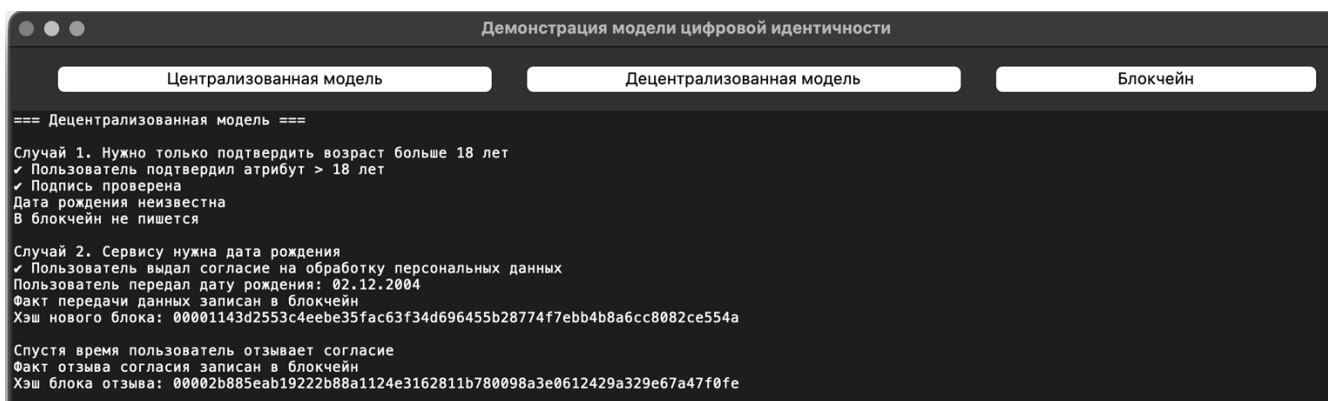


Рисунок 2. Демонстрация работы децентрализованной модели

Децентрализованная модель обеспечивает проверяемую историю обработки атрибутов, позволяя определить факт и время доступа веб-сервисов, а также выдачу и отзыв согласия.

Таким образом, в работе предложена децентрализованная модель цифровой идентичности пользователей веб-сервисов, основанная на использовании криптографически подтверждаемых атрибутов и протоколов доказательства знания. Такой подход позволяет подтверждать свойства пользовательских данных без

раскрытия их фактических значений и без необходимости централизованного хранения персональной информации.

Предложен механизм фиксации операций обработки атрибутов в распределённом реестре. Использование блокчейн-инфраструктуры позволяет формировать неизменяемую и проверяемую историю операций выдачи согласия и его отзыва, а также обеспечивает возможность последующего аудита использования персональных данных.

Результаты численного эксперимента демонстрирует практическую применимость модели и преимущество децентрализованной обработки данных, подтверждая возможность обеспечения конфиденциальности и прозрачности за счёт использования криптографических методов и распределённых реестров.

Литература

1. Бутакова Н.Г., Федоров В.Н. Криптографические методы и средства защиты информации: учебное пособие. – СПб: ИЦ «Интермедиа», 2020. – ISBN 978-5-4383-0210-0.
2. ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хэширования.- М., Стандартинформ, 2018.
3. ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.- М., Стандартинформ, 2012.

A DECENTRALIZED DIGITAL IDENTITY MODEL FOR WEB SERVICE USERS

student Tomchuk D.E.¹, Assoc. Prof., Ph.D. of Physico-mathematical Sciences Butakova N.G.^{1,2}

¹National Research University of Electronic Technology,

²Moscow Polytechnic University

The paper proposes a decentralized model of digital identity for web service users, enabling the verification of user attributes without the need for centralized storage of personal data. The model is based on the use of cryptographically verifiable attributes and zero-knowledge proof protocols, allowing the validation of specified conditions on attributes without revealing their actual values. In cases where a web service requires access to the full value of an attribute, a mechanism is provided for secure data transmission with cryptographic proof of authenticity and recording of data processing operations in a distributed ledger. The use of blockchain infrastructure ensures an immutable history of granting and revocation of consent for data processing and enables subsequent auditing of operations. An experimental software implementation has been developed to demonstrate the functionality of the proposed digital identity model.



ПРОТИВОДЕЙСТВИЕ ИНСАЙДЕРАМ В КОРПОРАТИВНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ

к.т.н., доц. Ушаков И.А.

Санкт-Петербургский государственный университет телекоммуникаций

Работа посвящена противодействию нарушителям в корпоративных компьютерных сетях, являющихся сотрудниками организаций. Кратко описывается модель признаков инсайдера, суть которой состоит в последовательном сборе от источников информации о сети индикаторов, продуцировании по ним индикаторов деятельности пользователей сети, вычислении стандартными способами агрегаторов и специализированными способами признаков, по которым делается формальное решение касательно наличия нарушителя. Дается обобщенное описание шагов метода выявления инсайдера (полное количество которых составляет 30), использующего данную модель и дополненного необходимыми действиями. Указываются нововведения в метод, отличающие его от аналогов. Приводятся обобщенные схемы модели и метода, а также указываются пути продолжения исследования.

[12] Введение

Инсайдеры в организациях представляют существенную угрозу информационной безопасности. Особую роль противодействие им носит в корпоративных компьютерных сетях, поддерживающих многопользовательскую работу и имеющих целый ряд специализированных служб. Несмотря на достаточно долгую историю противодействия таким внутренним нарушителям, проблема их наличия еще далека от завершения. Притом существующие способы, как правило, направлены на различные аспекты (или признаки) нарушителя – поведенческие и личностные [1], неумышленность действий [2], сбор информации вне должностных обязанностей [3] и пр. Одним же из путей эффективного обнаружения инсайдера может стать создание комплексного многошагового подхода, основанного на анализе больших объемов данных [4] и вынесении формального «вердикта» касательно нарушителя. И хотя подобные системы скорее всего будут основаны на использовании искусственного интеллекта, итоговое же решение может быть все также приниматься экспертом. Соответствующей аналитической модели признаков и методу выявления инсайдера в корпоративной компьютерной сети и посвящена текущая статья.

[13] Модель признаков инсайдера

Ранее автором была предложена модель признаков инсайдера, имеющая аналитический вид. Модель представляет собой вычислительная аппарат для вынесения решения касательно наличия инсайдера в организации. Обобщенная схема модели и окружения, необходимого для ее работы, представлены на рисунке 1.

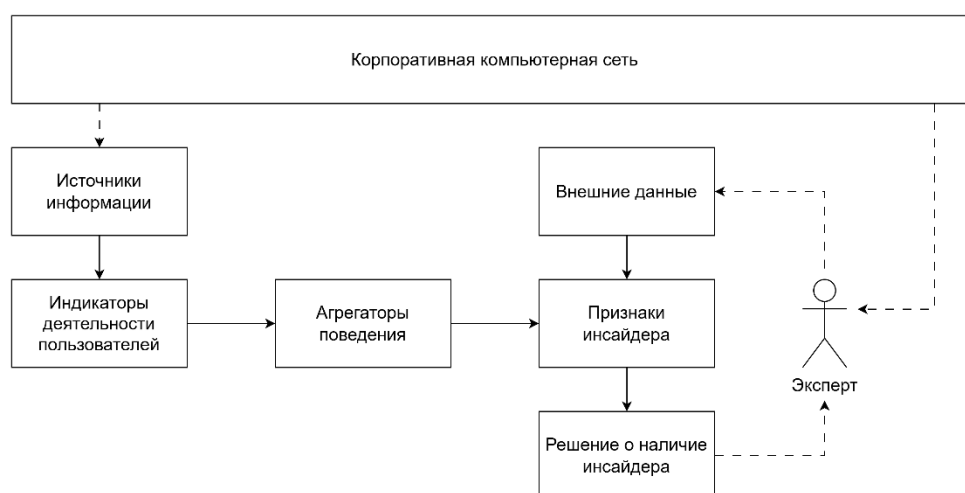


Рисунок 1 – Обобщенная схема модели признаков инсайдера

Дадим ряд пояснений касательно назначения и функционирования элементов модели (рисунок 1).

Основным «поставщиком» данных о поведении пользователей в организации является корпоративная компьютерная сеть, которая в рамках моделирования инсайдера представляет собой набор различных

информационных потоков, действий с ресурсами и иными объектами, свойства такого рода деятельности и т.п.

В такой корпоративной компьютерной сети выделены 5 различных источников информации, отражающих такие аспекты пользовательской активности, как 1) обмен данными через сеть внутри организации и с внешней средой, 2) непосредственная аутентификация пользователей в сети и ее службах, 3) доступ к сети организации и ее службам из внешней среды, 4) функционирование программно-аппаратных элементов на конечных устройствах и 5) производимые операции с файлами в организации (включая работу с базами данных).

Каждый из источников после сбора информации продуцирует целый набор индикаторов пользовательской активности, общее количество которых составляет 50. Так, например, первый источник предоставляет (но не ограничиваясь ими) такие индикаторы, как сетевые адреса источников и назначения, размер и время жизни пакета; второй – идентификатор пользователя и имя его учетной записи, а также, время входа в систему; третий – адрес, с которого был произведен удаленный доступ, диапазон удаленной работы; четвертый – идентификатор и тип устройства, свойства его процессов (имя, хэш); пятый – свойства файлов (имя, директория, хэш, размер и т.п.), запросы к базе данных и ответы от нее.

Затем, используя данные идентификаторов, по ним вычисляются значения-агрегаторы, представляющие более содержательную информацию о различных аспектах деятельности пользователей. Было выделено 30 агрегаторов, таких, как количество успешных и неудачных входов в систему, типы сетевой активности и характеристики соответствующего информационного обмена, временные характеристики работы пользователя в компьютерной сети (как внутри нее, так и в случае удаленного доступа), работа с конфиденциальными данными, сеансы и механизмы удаленного доступа к ресурсам сети и др. Способы вычисления агрегаторов по индикаторам являются типовыми, используемыми при обработке массивов данных; как правило, они относятся к статистическим. Так, например, по количеству попыток входа в систему можно составить распределение их результатов (вошел, неверный логин, неверный пароль); это, очевидно, в последствии позволит разделить сценарии, когда пользователь ошибся при вводе пароля, или злоумышленник пытается подобрать пароль.

Несмотря на то, что агрегаторы уже содержат значения, которые частично и только в совокупности могут быть использованы для выявления инсайдерской деятельности, тем не менее, четкого разделения пользователей на легальные и злонамеренные они сделать не позволят. Поэтому, в рамках модели и с использованием способов, специализированных на задачи исследования, по агрегаторам вычисляются непосредственные признаки инсайдера, каждый из которых определяет соответствующий уровень злонамеренной деятельности. Всего было выделено 15 признаков [5], таких, как попытки несанкционированного доступа (в системы в целом или к ее отдельным ресурсам), нестандартные шаблоны сетевого обмена, нарушения типичного времени работы пользователя в компании и пр. Так, например, первый из приведенных признаков вычисляется по количеству попыток входа в систему, используемых для этого устройствам и осуществляемым запросам. Для вычисления второго признака помимо запросов к ресурсам должна учитываться сетевая активность. А в случае третьего признака, он вычисляется на основании диапазона и распределения активности вне регламентированного в организации, а также, количества таких расхождений.

Наличие значений признаков (которые в общем случае представляют собой не отдельные числовые данные, а их кортежи или более сложные структуры) позволяет выносить соответствующие решения касательно наличия инсайдера в корпоративной компьютерной сети. Собственно, это и является основным результатом применения аналитической модели. Способов вынесения решений на основании набора признаков, очевидно, может быть несколько, среди которых (по мере усложнения) были выделены следующие: «порог» – превышение одним из признаков заданного значения; «счетчик превышений» – суммарное превышение несколькими признаками заданного предела; «взвешенная сумма» – суммирование всех признаков с учетом важности (веса) каждого и сравнение с заданным интегральным пределом; «классификатор» – применение машинного обучения для определения по совокупности признаков (входных данных для классификатора) класса пользователя (одним из которых будет нарушитель); «языковая модель» – применение более сложных технологий искусственного интеллекта на основе глубокого обучения с целью более «осмысленного» понимания поведения пользователей и ведения диалога с экспертом для выявления среди них инсайдеров.

Исходя из сложности задачи, «выводы» модели очевидно могут быть ошибочны по целому ряду причин – от ее несовершенности (например, отсутствуют необходимые индикаторы) до неполноты собранных данных (например, статистика попыток аутентификации собрана за час вместо дня). Таким образом, безусловное принятие мер противодействия инсайдеру (вплоть до увольнения сотрудника или заведения уголовного дела) на основе аналитических вычислений может иметь негативные последствия в случае ошибочности решения. Таким образом, итоговые решения модели целесообразно подвергать

экспертной оценке, а в случае необходимости саму модель дорабатывать или адаптировать к специфике работы в конкретной организации и ее корпоративной компьютерной сети.

[14] Метод выявления инсайдера

Наличие аналитической модели признаков хотя и позволяет теоретически определять инсайдера в организации, однако для практического применения требует ряда предварительных, промежуточных и финализирующих действий. В интересах этого был синтезирован соответствующий метод выявления инсайдеров, состоящий из 30 шагов, часть из которых (вне вычислений на основе модели) должна выполняться экспертом. Обобщенная схема метода представлена на рисунке 2; ККС – сокращение от «корпоративная компьютерная сеть», прямые линии указывают на функциональные связи, а пунктирные – на обмен основными данными.

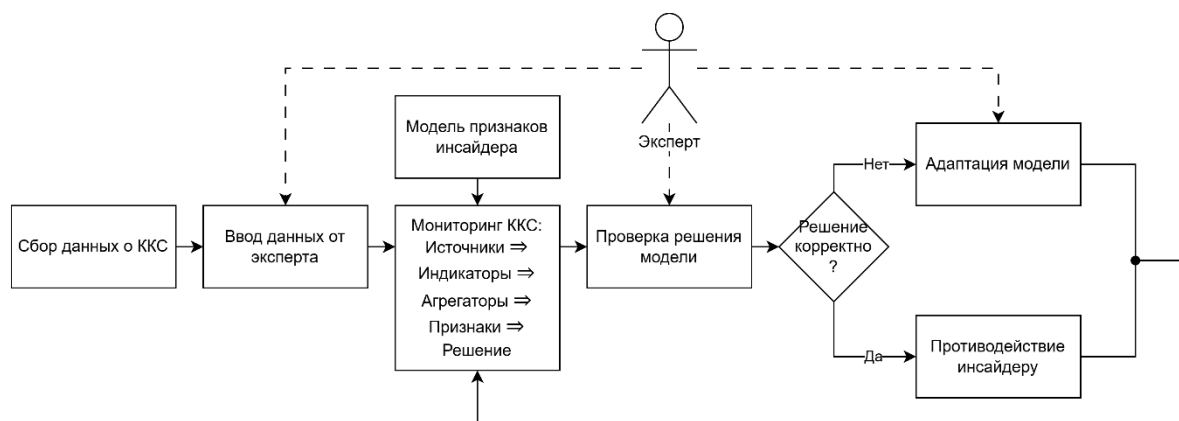


Рисунок 2 – Обобщенная схема метода выявления инсайдера

Суть метода (см. рисунок 2) заключается в следующем. Вначале производится сбор данных о корпоративной компьютерной сети, что позволяет сформировать доступный состав источников информации, их индикаторов и, как следствие, агрегаторов и признаков. Для этого, в частности, может привлекаться эксперт (а также, их группа, или целый выделенный отдел), обладающий более глубокими и точными знаниями об организации. Затем формируется модель признаков инсайдера, предназначенная для конкретной организации. После этого осуществляется основной этап работы с моделью, а именно – мониторинг корпоративной компьютерной сети путем последовательного получения (на схеме для этого указан знак «=>») из источников информации индикаторов, агрегаторов, признаков и решения. После формирования моделью решений, они периодически или событийно проверяются экспертом, а в случае обнаружения инсайдера осуществляются соответствующие мероприятия по противодействию инсайдеру. В случае, если эксперт посчитал, что решение моделью является некорректным (или даже недостаточно обоснованно), он производит ее доработку (т.е. адаптацию к условиям функционирования), например, введением новых индикаторов, настройкой операций по вычислению агрегаторов, расширением признаков или изменением способов принятия решений касательно инсайдера (например, дообучением классификатора или метода выявления аномалий [6]).

Для практической применимости модели, в типовую схему метода были внедрены следующие шаги, специализированные для задачи исследования: представление индикаторов, как кортежей или наборов числовых (иных) значений, собираемых источниками за некоторый промежуток времени; применение скользящего окна значений индикаторов для применения статистических (регрессионных) функций их обработки; для обеспечения непрерывности мониторинга расчет агрегаторов по частично собранным значениям индикаторов; оценка достоверности решений модели для более обоснованного их принятия экспертом; аналогично, интерпретация и объяснение решения, принятого моделью или ее интеллектуальными элементами [7].

[15] Заключение

В работе приведены начальные этапы исследования, направленного на выявление инсайдера в корпоративной компьютерной сети организации. Предложенная модель позволяет выносить формальные решения касательно наличия нарушителя, а метод их выявления указывает на основные шаги по подготовке и использованию модели, а также обработке их результатов. Новизна результатов исследования заключается

как в авторской аналитической модели, так и многошаговом методе и ряде нововведений в него; их более детальное описание находится в стадии публикации в научных журналах (на момент начала мая 2026 года). Продолжением исследования должно стать доведение модели и метода до реализации в виде соответствующих программных средств, а также их апробация на практике. Также, исходя из современного тренда в применении больших языковых моделей в области информационной безопасности [8], целесообразно их внедрение для интеллектуализации данной задачи.

[16] Литература

1. Власов Д.С. К вопросу о признаках инсайдерской деятельности // Национальная безопасность и стратегическое планирование. 2024. № 1 (45). С. 35-45. DOI: 10.37468/2307-1400-2024-1-35-45
2. Моисеенко Г.Ю. Метод противодействия неумышленному инсайдингу путем повышения устойчивости инструкций по работе в информационной системе // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2025. № 4. С. 107-116. DOI: 10.61260/2218-130X-2025-4-107-116
3. Фадюшин С.Г. Разработка метода диагностики риска инсайдерских угроз // Современные наукоемкие технологии. 2023. № 2. С. 111-115. DOI: 10.17513/snt.39531
4. Смирнов Д.В., Грушо А.А., Забежайло М.И., Тимонина Е.Е. Система сбора и анализа информации из различных источников в условиях Big Data // International Journal of Open Information Technologies. 2021. Т. 9. № 4. С. 64-71.
5. Ушаков И.А. Обоснование демаскирующих признаков инсайдеров в корпоративных компьютерных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2024. № 3. С. 95-106. DOI: 10.46418/2079-8199_2024_3_
6. Поляничко М.А. Методика обнаружения аномального взаимодействия пользователей с информационными активами для выявления инсайдерской деятельности // Труды учебных заведений связи. 2020. Т. 6. № 1. С. 94-98. DOI: 10.31854/1813-324X-2020-6-1-94-98
7. Аверкин А.Н. Объяснимый искусственный интеллект как часть искусственного интеллекта третьего поколения // Речевые технологии. 2023. № 1. С. 4-10.
8. Abdennebi A., Nadja K., Lahlou L., Younis M., Ould-Slimane H. Sec-Llama: a Compact Fine-Tuned LLM for Network Intrusion Detection in Kubernetes Clusters // The proceedings of IEEE International Conference on Machine Learning for Communication and Networking (26-29 May 2025, Barcelona, Spain). 2025. PP. 1-7. DOI: 10.1109/ICMLCN64995.2025.11140090.

COUNTERING INSIDERS IN CORPORATE COMPUTER NETWORKS

Ph.D., Associate Professor, I.A. Ushakov

The Bonch-Bruевич Saint-Petersburg State University of Telecommunications

This paper focuses on countering intruders in corporate computer networks who are employees of organizations. It briefly describes a model of insider indicators, which consists of sequentially collecting indicators from network information sources, generating user activity indicators based on these indicators, and calculating indicators using standard aggregator methods and specialized methods, which formally determine the presence of an intruder. A summary of the steps of the insider detection method (30 in total) using this model is provided, supplemented with necessary actions. Innovations in the method that distinguish it from similar approaches are highlighted. Generalized diagrams of the model and method are presented, along with directions for further research.



ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ РАЗБОРЧИВОСТИ РЕЧИ В УСЛОВИЯХ ПОМЕХ

проф. Хорев А.А.

Национальный исследовательский университет «МИЭТ»

В статье представлены результаты экспериментальных исследований разборчивости зашумленных речевых сигналов. В качестве помеховых сигналов использовались: «белый» шум, «розовый» шум, шумовая «речеподобная» помеха и помеха типа «речевой хор». В качестве исходных тестовых речевых сигналов использовались артикуляционные таблицы односложных слов. Для чтения таблиц были привлечены 6 дикторов. Для формирования шумовых сигналов использовалась ПЭВМ и специальное программное обеспечение Adobe Audition 1.5. Шумовая помеха типа «речевой хор» была сформирована из смеси речевых сигналов (таблиц фраз) пяти дикторов, при этом при формировании помехи паузы между словами из записей удалялись. Для каждого вида шумового сигнала были сформированы аудиофайлы с отношениями сигнал/шум от -20 до $+10$ дБ с шагом в 2 дБ. Экспериментальные исследования разборчивости зашумленных речевых сигналов проводила бригада auditors в составе 8 человек в возрасте от 20 до 23 лет. В результате экспериментальных исследований для каждого вида шума получены аналитические соотношения, позволяющие рассчитать словесную разборчивость речи в зависимости от отношения сигнал/шум.

Введение

В качестве показателя эффективности защиты акустической речевой информации используется словесная разборчивость речи, под которой понимается относительное количество правильно понятых человеком слов из перехваченного разговора [1].

Для оценки словесной разборчивости речи используется методика [1], в основу которой положены экспериментальные исследования профессора Н.Б. Покровского [2].

Исследования разборчивости речи профессором Н.Б.Покровским проводились только в условиях «белого» шума. Поэтому целью данных экспериментальных исследований служит оценка разборчивости речевых сигналов, зашумленных следующими видами шумов: «белый» шум – шум с равномерной спектральной плотностью; «розовый» шум – шум со спадом спектральной плотности 3 дБ/на октаву; шумовая «речеподобная» помеха – шум с огибающей спектра, подобной огибающей речевого сигнала; помеха типа «речевой хор» – помеха, формируемая из смеси речевых сигналов пяти дикторов.

1. Формирование зашумленных тестовых речевых сигналов

При проведении экспериментальных исследований в качестве исходных тестовых речевых сигналов использовались артикуляционные таблицы односложных слов [3].

Запись исходных тестовых речевых сигналов проводилась в служебном помещении при уровне шума не более 35 - 40 дБ бригадой из 6-ти дикторов (4 мужчины и 2 женщины), не имеющих дефектов речи. Запись проводилась на цифровой диктофон (портативный рекордер) Tascam DR-100. Режим записи: 44.1 кГц, 24 бит, формат записи – wav. Запись проводилась на съемную SD – карту. Чтение слов и фраз дикторами осуществлялось ровным голосом, четко, но без подчеркивания отдельных звуков с постоянным уровнем речи. Дикторы выдерживали постоянный ритм речи на протяжении чтения всей таблицы.

Для формирования «белого», «розового» шумов, шумовой «речеподобной» помехи и помехи типа «речевой хор» использовалась ПЭВМ и специальное программное обеспечение Adobe Audition 1.5 [4].

Формирование зашумленных тестовых речевых сигналов с заданным отношением сигнал/шум проводилось в следующей последовательности:

Из каждого аудиофайла с записью исходного тестового речевого сигнала удалялись паузы между словами. Удаление из аудиофайла пауз между словами осуществлялось в автоматическом режиме с использованием инструмента программы «Удалить тишину».

Для исключения нелинейных искажений производилась нормализация амплитуды сигналов с использованием опции «Эффекты – Амплитуда – Нормализация».

Учитывая, что частотный диапазон речевых сигналов ограничен частотой 11200 Гц, производилась конвертация аудиофайлов с использованием частоты дискретизации 22050 Гц и разрешения 16 бит.

С целью исключения нелинейных искажений при смешении исходных тестовых речевых сигналов с шумом при изменении отношения сигнал/шум в пределах от -20 дБ до $+10$ дБ экспериментально было установлено, что средний уровень тестового речевого (с вырезанными паузами) должен составлять -34 дБ.

Для изменения амплитуды сигналов использовался инструмент «Усиление/Затухание». Коэффициент усиления экспериментально подбирался таким образом, что бы средний уровень речевого сигнала (с вырезанными паузами) был равен -34 дБ. Уровень сигнала проверялся с помощью инструмента «Статистика». Уровень сигнала -34 дБ обеспечивался при коэффициенте усиления $-5,69$ дБ.

Далее такой же коэффициент усиления (– 5,69 дБ) устанавливается и для тестового речевого сигнала с паузами, после чего измерялся его средний уровень. Разница средних уровней исходных тестовых речевых сигналов без пауз и с паузами рассчитывался по формуле:

$$\Delta L = L_{с.бп} - L_{с.п}, \quad (1)$$

где $L_{с.бп}$ – средний уровень тестового речевого сигнала без пауз, дБ;

$L_{с.п}$ – средний уровень тестового речевого сигнала с паузами, дБ;

ΔL – разница средних уровней исходных тестовых речевых сигналов без пауз и с паузами, дБ.

Разница средних уровней исходных тестовых речевых сигналов без пауз и с паузами составляла более 11 дБ.

Для создания шумового сигнала типа «белый» шум использовался инструмент «Создание – Шум», цвет – «белый» шум, стиль – моно, частота дискретизации 22050 Гц, разрядность – 16 бит.

Процесс формирования «розового» шума отличается от процесса формирования «белого» шума только на этапе выбора вида шума: цвет – «розовый».

Шумовая «речеподобная» помеха формировалась из «белого» шума путем изменения его огибающей спектра с использованием графического десяти полосового эквалайзера (инструмент «Эффекты» – «Фильтры» – «Графический эквалайзер»).

Шумовая помеха типа «речевой хор» была сформирована из смеси речевых сигналов пяти дикторов. В качестве исходных речевых сигналов использовались записи таблиц фраз [5]. При этом при формировании помехи паузы между словами из записей удалялись.

Средний уровень создаваемого шума (для каждого вида шума) измерялся с помощью инструмента «Статистика».

Уровень шума $L_{ш}$, необходимый для создания требуемого отношения сигнал/шум (q) рассчитывался по формуле:

$$L_{ш} = L_{с.п} + \Delta L - q, \quad (2)$$

где ΔL – разница средних уровней исходных тестовых речевых сигналов без пауз и с паузами, рассчитываемая по формуле (1), дБ;

q – отношение сигнал/шум, дБ.

Уровень шума для создания требуемого отношения сигнал/шум устанавливался с помощью инструмента «Усиление/Затухание».

При проведении экспериментальных исследований под отношением сигнал/шум понималось среднее отношение речевой сигнал/шум за весь период воспроизведения диктором артикуляционной таблицы.

Формирование зашумленных тестовых речевых сигналов осуществлялось путем смешения речевых сигналов с шумовыми. Для каждого вида шумового сигнала были сформированы аудиофайлы с отношениями сигнал/шум от – 20 до +10 дБ с шагом в 2 дБ.

С целью оценки корректности формирования зашумленных речевых сигналов с использованием программного обеспечения Adobe Audition 1.5 были проведены экспериментальные исследования, методика проведения которых заключалась в следующем:

- акустическая колонка «Behringer EUROLIVE B208D» и шумомер «ЭКОФИЗИКА-110А» устанавливались на стойки. Расстояние от микрофонного капсюля шумомера до плоскости динамика акустической колонки составляло 1 м;
- к линейному входу акустической колонки кабелем Jack–Jack (3,5 мм) подключается звуковая карта ноутбука;
- на ноутбуке запускается аудиофайл (аудиозапись) исходного тестового речевого сигнала (без пауз) и с использованием шумомера в режиме «ЭкоЗвук» измеряется уровень звукового давления в октавных полосах.
- на ноутбуке запускается аудиофайл (аудиозапись) шумового сигнала, генерируемого программой «Adobe Audition 1.5», и с использованием шумомера в режиме «ЭкоЗвук» измеряется уровень звукового давления в октавных полосах.

При измерениях в качестве тестовых речевых сигналов использовалась артикуляционная таблица односложных слов. Из аудиофайла с записью исходного тестового речевого сигнала удалялись паузы между словами.

Измерения проводились для зашумленных тестовых речевых сигналов с отношением сигнал/шум: – 10 дБ, 0 дБ и +10 дБ.

В качестве шумового сигнала использовались: «белый» шум, «розовый» шум, «речеподобная» шумовая помеха и помеха типа «речевой хор».

Расчет отклонения отношения сигнал/шум, рассчитанного в программе «Adobe Audition 1.5», от отношения сигнал/шум, рассчитанного по результатам измерений проводился по формуле:

$$\Delta q = q - q_э = q - (L_c - L_{ш}), \quad (3)$$

где q – отношение сигнал/шум, рассчитанное в программе «Adobe Audition 1.5», дБ;

$q_э$ – отношение сигнал/шум, рассчитанное по результатам измерений, дБ;

L_c – измеренный интегральный уровень речевого сигнала, дБ;

$L_{ш}$ – измеренный интегральный уровень шумового сигнала, дБ.

Анализ полученных данных измерений показывал, что для «розового» шума, шумовой «речеподобной» помехи и помехи типа «речевой хор» среднее отклонение Δq составляет от + 0,7 до – 1,9 дБ, что с учетом погрешности измерений уровня сигналов шумомером ($\pm 2,0$ дБ) является весьма приемлемым результатом.

Для белого шума это отклонение составляет – 3,03 дБ, что превышает погрешность измерений уровня сигналов шумомером ($\pm 2,0$ дБ).

2. Экспериментальные исследования разборчивости зашумленных речевых сигналов

Экспериментальные исследования разборчивости зашумленных тестовых речевых сигналов проводила бригада аудиторов в составе 8 человек в возрасте от 20 до 23 лет. Все аудиторы не имели дефектов слуха.

Для прослушивания аудиторам предъявлялись аудиофайлы с записями зашумленных речевых сигналов. Для прослушивания зашумленных речевых сигналов использовались ПЭВМ и медиаплеер VLC. Прослушивание сигналов осуществлялось аудитором через головные наушники AKG K271 MKII, подключаемые к линейному выходу звуковой карты ПЭВМ.

Каждый аудитор для каждого вида шума прослушивал по 1 таблице слов (50 слов). Для каждого вида шума использовались разные таблицы слов.

Аудиторы прослушивали аудиофайлы с записью зашумленных тестовых речевых сигналов с отношением сигнал/шум от – 20 до +10 дБ с шагом 2 дБ. Для каждого вида шума прослушивание аудиофайлов начиналось с файла с наименьшим отношением сигнал/шум $q = -20$ дБ и заканчивается аудиофайлом с максимальным значением отношения сигнал/шум $q = +20$ дБ.

После прослушивания каждого слова аудитор останавливал воспроизведение записи и заносил услышанное слово в таблицу. При сложности восприятия разрешается аудитор мог отматывать запись назад и повторно прослушивать слово (фразу).

На прослушивание аудиофайлов для одного вида шума с отношением сигнал/шум от – 20 до +10 дБ с шагом 2 дБ (16 аудиофайлов) одним аудитором уходило от 2,5 до 3 часов.

В результате обработки результатов распознавания зашумленных слов для каждого вида помехи и отношения сигнал/шум рассчитывалась словесная разборчивость речи для каждого аудитора (k):

$$W_{jik} = N_{jik}/N, \quad (4)$$

где W_{jik} – словесная разборчивость речи аудиофайла для j -го вида помехи и i -го отношения сигнал/шум, определенная k -м аудитором;

N_{jik} – количество правильно распознанных k -м аудитором слов в аудиофайле для j -го вида помехи и i -го отношения сигнал/шум (слово считалось правильно понятым, если аудитор правильно его написал);

N – общее количество слов в аудиофайле для j -го вида помехи и i -го отношения сигнал/шум ($N=50$).

Далее рассчитывалась средняя разборчивость речи по всем аудиторам:

$$W_{ji} = \frac{\sum_{k=1}^K W_{jik}}{K}, \quad (5)$$

где W_{ji} – средняя словесная разборчивость речи для j -го вида помехи и i -го отношения RMS ;

K – общее количество аудиторов.

Предварительный анализ полученных результатов словесной разборчивости речи показал, что ее зависимость от отношения сигнал/шум достаточно точно аппроксимируется зависимостью:

$$W = \Phi(Q_1 \cdot q - Q_2), \quad (6)$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^x \exp\left(-\frac{t^2}{2}\right) dt$ – интеграл вероятности;

q – отношение сигнал/шум, дБ;

Q_1 и Q_2 – коэффициенты, зависящие от вида сигнала (слова, фразы), вида шума и индивидуальных особенностей слушателей.

Выбор значений коэффициентов Q_1 и Q_2 для каждого вида шума проведем из условия, при котором достоверность аппроксимации максимальна:

$$\{Q_1; Q_2\} \rightarrow \max R^2, \quad (7)$$

где $R^2 = 1 - \frac{\sum_{i=1}^N (W_i - W_{i,3})^2}{\sum_{i=1}^N (W_{i,3})^2 - \frac{1}{N} (\sum_{i=1}^N W_{i,3})^2}$ – характеризует достоверность аппроксимации [6]; W_i –

словесная разборчивость речи для i -го отношения сигнал/шум, рассчитанная по формуле (6);

$W_{i,3}$ – словесная разборчивость речи для i -го отношения сигнал/шум, рассчитанная по формуле (4) или (5);

N – количество значений отношений сигнал/шум для которых проводились экспериментальные исследования (в нашем случае $N = 16$).

Для расчета значений коэффициентов Q_1 и Q_2 и построения аппроксимирующей кривой разработана специальная программа, написанная на языке программирования Python 3.5.

Рассчитанные значения коэффициентов Q_1 и Q_2 и ошибки аппроксимации, рассчитанные для формулы (5) приведены в таблице 1.

Таблица 4

Рассчитанные значения коэффициентов Q_1 и Q_2 (для 8 слушателей)

Вид помехи	Q_1	Q_2	R^2
«Белый» шум	0,10	– 0,30	0,996
«Розовый» шум	0,13	– 0,37	0,994
«Шумоподобная» речеподобная помеха	0,12	– 0,38	0,991
Помеха типа «речевой хор»	0,13	– 0,19	0,995

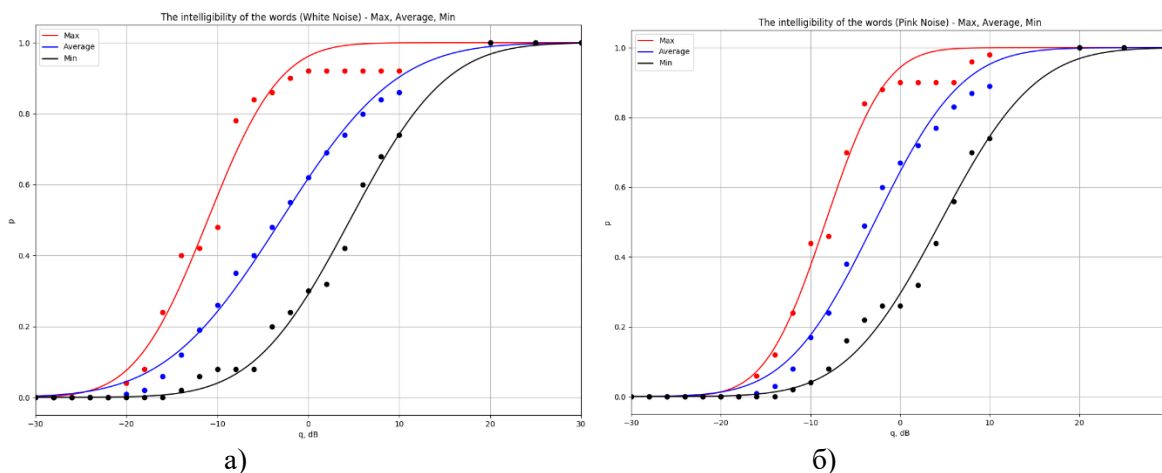


Рисунок 1 – Графики зависимости словесной разборчивости речи от отношения сигнал/шум: «белый» шум (а), «розовый» шум (б)

На рисунках 1 и 2 приведены графики зависимости словесной разборчивости речи от отношения сигнал/шум, построенные по аппроксимирующей формуле (5) для максимальных (max), минимальных (min) и средних ($average$) значений разборчивости речи. Точками на графиках показаны данные, полученные по результатам артикуляционных испытаний.

Анализ графиков, представленных на рисунке 1 и риунке 2, показывает, что:

наблюдается существенный разброс значений разборчивости речи при одних и тех же значениях отношений сигнал/шум. Например, для «белого» шума при отношении $q = 0$ дБ у разных слушателей разборчивость речи составляла от 30% до 90%, при среднем значении около 60%, что говорит о том, что несмотря на нормальный слух, не все слушатели способны распознавать зашумленные речевые сигналы;

при низких отношениях сигнал/шум наиболее эффективной из рассматриваемых видов помех является помеха типа «речевой хор».

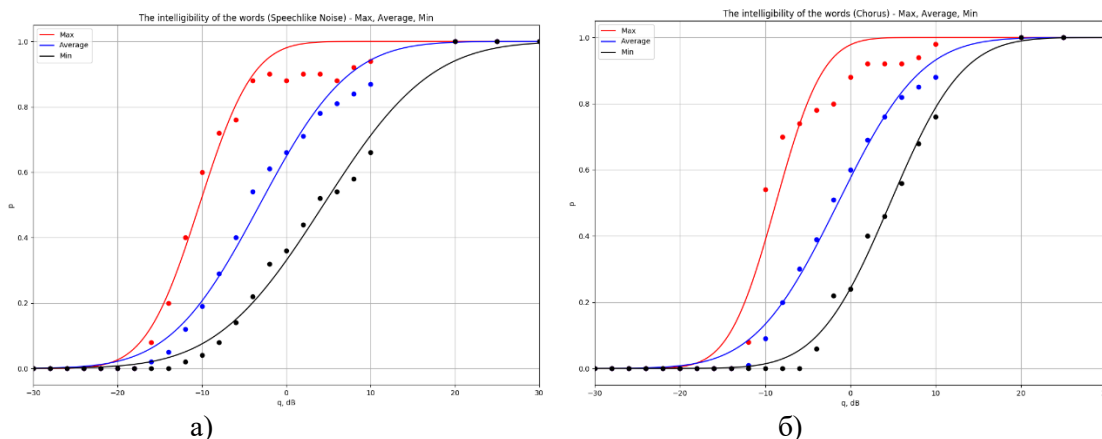


Рисунок 2 – Графики зависимости словесной разборчивости речи от отношения сигнал/шум: шумовая «речеподобная» помеха (а), помеха типа «речевой хор» (б)

На рисунке 3 («а», «б») приведены графики зависимости словесной разборчивости речи от отношения RMS , построенные по аппроксимирующей формуле (5) для средних (*average*) значений разборчивости речи и значений коэффициентов Q_1 и Q_2 , приведенных в таблице 4, и рассчитанные по формантной методике разборчивости речи [1].

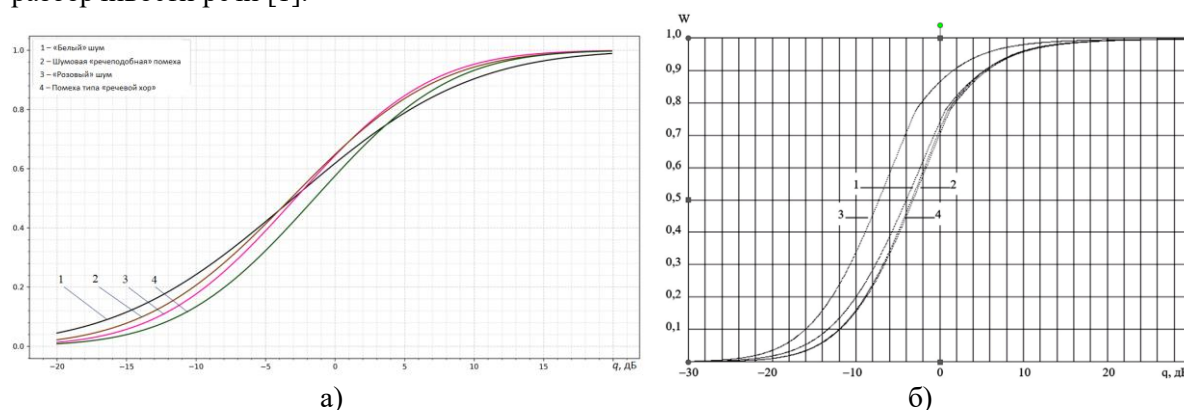


Рисунок 3 – Графики зависимости словесной разборчивости речи от отношения сигнал/шум: а)– построенные по формуле (5) для средних (*average*) значений разборчивости речи; б) – рассчитанные по формантной методике разборчивости речи [1]

Анализ полученных результатов показывает, значения словесной разборчивости речи, рассчитанные по формантной методике разборчивости речи, несколько выше средних значений, полученных по результатам артикуляционных испытаний, но не выходят за их максимальные значения. Возможно, эти отличия объясняются тем фактом, что при проведении артикуляционных испытаний использовались очень короткие слова (в основном состоящие из одного слога), с которыми аудиторы в своей деятельности не встречались и смысл некоторых из них им был непонятен.

Заключение

Анализ полученных результатов артикуляционных испытаний позволяет сделать следующие выводы:

разборчивость речи в значительной степени зависит от того факта, знакомы ли слова, входящие в артикуляционную таблицу, аудитору, или нет. Если слова известны, то словесная разборчивость значительно возрастает. Следовательно, с целью оценки разборчивости речи в интересах защиты речевой информации необходимо разработать артикуляционные таблицы ключевых слов по различным классам (областям) знаний;

разборчивость речи существенно зависит от особенностей восприятия зашумленных речевых сигналов аудиторами. При одинаковых отношениях сигнал/шум разборчивость речи для разных аудиторов может отличаться на десятки процентов. Например, для «белого» шума при отношении $q = 0$ дБ словесная разборчивость для различных аудиторов отличалась от среднего значения (60%) в пределах от + 30% до + 30%. Следовательно, для оценки разборчивости речи в интересах защиты речевой информации методом артикуляционных испытаний необходимо привлекать подготовленных аудиторов, обладающих способностью распознавать речь при низких отношениях RMS .

словесная разборчивость речи близка к нулю для всех видов помех при отношении $q < -25$ дБ.

Литература

1. Хорев А.А. Оценка возможностей средств акустической (речевой) разведки//Специальная техника. – М.: 2009. – № 4 – С. 49-63.
2. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Гос. Издательство литературы по вопросам связи и радио, 1962, - 392 с.
3. ГОСТ 16600-72. Передача речи по трактам связи радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений. – Введ. 1972-09-27. М.: Государственный комитет стандартов совета министров СССР, 1972. – 93 с.
4. Adobe AUDITION 1.5: Руководство пользователя. [Электронный ресурс]. – Режим доступа: <https://www.manualslib.com/manual/1995/Adobe-Audition-1-5.html>.
5. ГОСТ Р 50840-95. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. – Введ. 1997-01-01. – М.: Изд-во стандартов, 1996. – 202 с.
6. Малышева Т.А. Численные методы и компьютерное моделирование. Лабораторный практикум по аппроксимации функций. [Электронный ресурс]. – Режим доступа: <http://books.ifmo.ru/file/pdf/1953.pdf>.

EXPERIMENTAL STUDIES OF SPEECH INTELLIGIBILITY UNDER INTERFERENCE CONDITIONS

Prof. Horev A.A.

National Research University of Electronic Technology

The article presents the results of experimental studies of the intelligibility of noisy speech signals. The following interference signals were used: "white" noise, "pink" noise, "speech-like" noise, and "speech chorus" type interference. Articulation tables of monosyllabic words were used as the initial test speech signals. 6 speakers were involved in reading the tables. A PC and special Adobe Audition 1.5 software were used to generate the noise signals. The "speech chorus" type noise interference was formed from a mixture of speech signals (phrase tables) from five speakers, while the pauses between words were removed from the recordings when the interference was formed. Audio files with signal-to-noise ratios (RMS) from -20 to $+10$ dB in 2 dB increments were generated for each type of noise signal. Experimental studies of the intelligibility of noisy speech signals were conducted by a team of auditors consisting of 8 people aged 20 to 23 years. As a result of experimental studies, analytical ratios have been obtained for each type of noise, which make it possible to calculate the verbal intelligibility of speech depending on the RMS ratio.



ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПОЛОСЫ ПРОПУСКАНИЯ ПРИЕМНОГО УСТРОЙСТВА НА РАЗБОРЧИВОСТЬ РЕЧИ ПРИ ПЕРЕХВАТЕ ИНФОРМАЦИИ МЕТОДОМ «ВЫСОКОЧАСТОТНОЙ НАКАЧКИ»

проф. Хорев А.А., студ. Чачилло Т.В.

Национальный исследовательский университет «МИЭТ»

В статье приведены результаты экспериментальных исследований зависимости словесной разборчивости речи от полос пропускания приемного устройства (RBW и VBW) при перехвате акустической речевой информации методом «высокочастотной накачки» телефонного аппарата. Исследования проводились для RBW – 30 Гц и 10 Гц и VBW – 30 кГц, 10 кГц и 3 кГц. При проведении экспериментальных исследований установлено, что словесная разборчивость речи на выходе аналогового демодулятора анализатора спектра при расположении антенны на удалении 1 м от телефонного аппарата не превышает 26,7% даже для очень громкой речи ($L = 84$ дБ). При использовании цифровых методов демодуляции сигналов словесная разборчивость речи может составлять: для громкой речи - более 22% на дальностях до 5 м; для очень громкой речи – более 20% на дальностях до 25 м. При этом, изменение полосы пропускания RBW не оказывает существенного влияния на разборчивость речи.

Канал утечки, создаваемый методом «высокочастотной накачки» технических средств (ТС), установленных в выделенном помещении (ВП), является одним из наиболее опасных технических каналов утечки акустической речевой информации.

В работе [1] приведены результаты экспериментальных исследований подверженности телефонного аппарата VEF TA-D» (TA611D) «высокочастотной накачке». В результате исследований установлено, что телефон подвержен ВЧ-накачке в диапазоне частот от 30 МГц до 270 МГц, а максимальный уровень напряженности поля информативного сигнала наблюдается на частоте 230 МГц.

Для измерения характеристик переизлученного телефонным аппаратом информативного высокочастотного сигнала использовался анализатор «Rohde&Schwarz FSH8» с чувствительностью (при RBW = 1 Гц) – 146 дБм. Измерения уровней информативных сигналов проводились на выходе полосового фильтра при отключенном предусилителе и полосе пропускания RBW = 30 Гц.

Цель данных исследований – оценить влияние полос пропускания RBW и VBW на разборчивость речи при перехвате информации методом «высокочастотной накачки» телефонного аппарата.

Для проведения экспериментальных исследований был создан лабораторный стенд в составе: телефонный аппарат «VEF TA-D»; генератор сигналов «Rohde&Schwarz SMB100A»; электрическая дипольная активная измерительная антенна П6-51; анализатор спектра «Rohde&Schwarz FSL3» с опциями R&S®FSL-B7, R&S®FSL-B22 и R&S®FSL-K7; акустическая система «BEHRINGER B208D»; генератор НЧ-сигналов «Agilent 33521A»; шумомер «Экофизика-110А»; селективный микровольтметр «B6-17».

Исследования проводились в три этапа.

На первом этапе проводились исследования влияния полосы пропускания RBW анализатора спектра на разборчивость речи.

Исследования проводились в соответствии с методикой, изложенной в [1].

В качестве тестового сигнала использовались гармонические колебания на среднегеометрических частотах пяти октавных полос: 250, 500, 1000, 2000 и 4000 Гц.

Измерения уровней информативных сигналов проводилось при двух значениях полосы пропускания RBW 30 и 10 Гц.

Пример спектрограмм переизлученного телефонным аппаратом сигналов приведен на рисунке 1.

Далее на основе результатов измерений уровней сигналов и шумов проводился расчет уровня информативного сигнала и отношения сигнал/шум в октавных полосах по формулам:

$$U_{c,i} = 10 \lg(10^{0,1U_{(c+\pi),i}} - 10^{0,1U_{\pi,i}}); \quad (1)$$

$$q_{c,i} = 20 \lg \left[\frac{10^{0,05 \cdot U_{c,i} \cdot \sqrt{RBW}}}{10^{0,05 \cdot U_{\pi,i} \cdot \sqrt{\Delta F_i}}} \right], \quad (2)$$

где $U_{c,i}$ – уровень информативного сигнала на среднегеометрической частоте i -й октавной полосы, дБ(мкВ);

$U_{(c+\pi),i}$ – уровень модуляционной составляющей при включенном тестовом сигнале на среднегеометрической частоте i -й октавной полосы, дБ(мкВ);

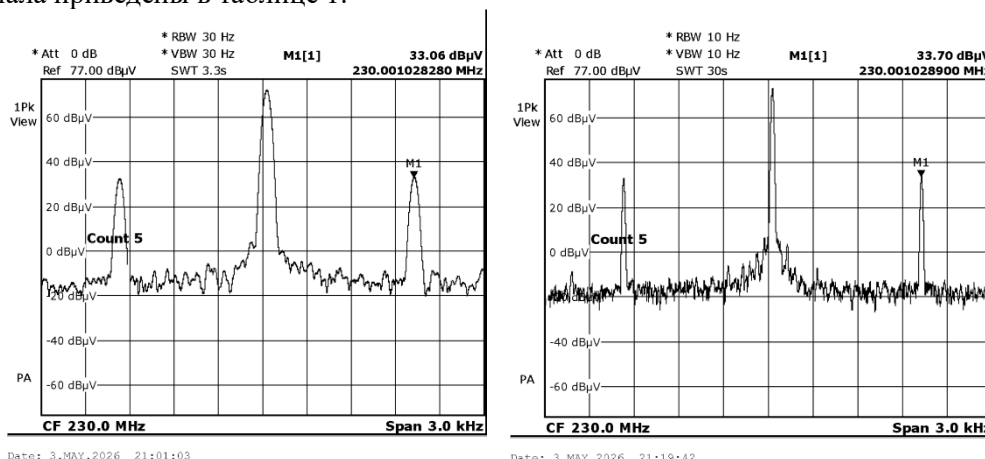
$U_{\pi,i}$ – уровень шумов при выключенном тестовом сигнале на среднегеометрической частоте i -й октавной полосы, дБ(мкВ);

$q_{c,i}$ – отношение сигнал/шум в i -й октавной полосы, дБ;

ΔF_i – ширина i -й октавной полосы, Гц;

RBW – ширина полосы пропускания на выходе полосового фильтра анализатора спектра, Гц.

Рассчитанные по формуле (2) отношения сигнал/шум в октавных полосах для максимальных уровней тестового сигнала приведены в таблице 1.



а)

б)

Рисунок 1. Спектрограммы переизлученных телефонным аппаратом модулированных высокочастотных сигналов (частота сигнала ВЧ-навязывания – 230 МГц, мощность генератора ВЧ-сигнала – 25 дБм, уровень тестового акустического сигнала – максимальный, частота тестового акустического сигнала – 1 кГц):
 $RBW = 30$ Гц (а), $RBW = 10$ Гц (б)

Таблица 1

Рассчитанные отношения сигнал/шум в октавных полосах

Номер октавной полосы (диапазон частот, Гц)	Уровень тестового акустического сигнала ($L_{u,i}$), дБ	Отношение сигнал/шум ($q_{c,i}$), дБ	
		$RBW = 30$ Гц	$RBW = 10$ Гц
2 (180 – 355)	109,8	19,3	17,2
3 (355 – 710)	110,5	24,5	29,1
4 (710 – 1420)	105,4	33,1	32,9
5 (1420 – 2840)	102,7	21,2	25,9
6 (2840 – 5680)	105,7	31,6	27,7

Отношения сигнал/шум, приведенные в таблице 1, рассчитаны для уровней тестового акустического сигнала, существенно превышающих уровни типовых речевых сигналов [2]. Проведенные исследования [1] показали, что при перехвате информации методом «высокочастотной накачки», отношение сигнал/шум на входе приемного устройства растет прямо пропорционально уровню тестового акустического сигнала. Следовательно, для расчета отношения сигнал/шум, соответствующего типовым значений уровней сигналов в октавных полосах, приведенных в [2], можно рассчитать по формуле:

$$q_{c,m,i} = q_{c,i} - \Delta L = q_{c,i} - (L_{u,i} - L_{c,i}), \quad (3)$$

где $q_{c,m,i}$ – отношение сигнал/шум для i -й октавной полосы, соответствующее типовому спектру речевого сигнала, дБ;

$q_{c,i}$ – отношение сигнал/шум для i -й октавной полосы, соответствующее уровню тестового акустического сигнала, дБ;

$L_{u,i}$ – измеренный уровень громкости тестового сигнала в i -й октавной полосе, дБ;

$L_{c,i}$ – типовой уровень громкости речевого сигнала в i -й октавной полосе, дБ.

Расчет словесной разборчивости речи, проведенной в соответствии с методикой, приведенной в [2] показал, что словесная разборчивость речи составляет:

для речи средней громкости ($L = 70$ дБ): 8,3% ($RBW = 30$ Гц); 8,5% ($RBW = 10$ Гц);

для громкой речи ($L = 76$ дБ): 27,1% ($RBW = 30$ Гц); 28,5% ($RBW = 10$ Гц);

для очень громкой речи ($L = 84$ дБ): 71,4% ($RBW = 30$ Гц); 74,4% ($RBW = 10$ Гц).

Следовательно, изменение полосы пропускания RBW не оказывает существенного влияния на разборчивость речи, но при полосе пропускания $RBW = 10$ Гц разборчивость речи несколько выше, чем при $RBW = 30$ Гц.

На втором этапе проводились исследования влияния полосы пропускания VBW анализатора спектра на разборчивость речи.

Исследования также проводились в соответствии с методикой, изложенной в [1]. Однако измерения проводились не на выходе полосового фильтра, а на выходе аналогового демодулятора с использованием селективного микровольтметра В6-17 при его полосе пропускания $\Delta F = 10$ Гц.

Измерения уровней информативных сигналов проводилось при трех значениях полосы пропускания VBW: 30 кГц, 10 кГц и 3 кГц.

Внешний вид экрана селективного микровольтметра В6-17 при измерении уровней модуляционных составляющих тестовых сигналов приведен на рисунке 2.

Рассчитанные по формуле (2) отношения сигнал/шум в октавных полосах на аналоговом выходе демодулятора для максимальных уровней тестового сигнала приведены в таблице 2.



Рисунок 2. Внешний вид экрана селективного микровольтметра В6-17 при измерении уровней модуляционных составляющих тестовых сигналов (частота сигнала ВЧ-навязывания – 230 МГц, мощность генератора ВЧ-сигнала – 25 дБм, уровень тестового акустического сигнала – максимальный, частота тестового акустического сигнала – 4 кГц): VBW= 30 кГц (а), VBW= 10 кГц (б), VBW=3 кГц (в)

Таблица 2

Рассчитанные отношения сигнал/шум в октавных полосах

Номер октавной полосы (диапазон частот, Гц)	Уровень тестового акустического сигнала ($L_{u,i}$), дБ	Отношение сигнал/шум (q_{ci}), дБ		
		$VBW = 30$ кГц	$VBW = 10$ кГц	$VBW = 3$ кГц
2 (180 – 355)	109,8	7,91	9,42	8,61
3 (355 – 710)	110,5	15,79	16,60	20,50
4 (710 – 1420)	105,4	11,11	16,11	10,01
5 (1420 – 2840)	102,7	23,64	20,14	18,14
6 (2840 – 5680)	105,7	20,63	20,13	-27,37

Расчет, выполненный в соответствии с методикой, приведенной в [2], показал, что словесная разборчивость речи составляет:

для речи средней громкости ($L = 70$ дБ): 1,0 % ($VBW = 30$ кГц); 0,4 % ($VBW = 10$ кГц) и 0,2% ($VBW = 3$ кГц);

для громкой речи ($L = 76$ дБ): 5,2 % ($VBW = 30$ кГц); 2,8 % ($VBW = 10$ кГц) и 1,3% ($VBW = 3$ кГц);

для очень громкой речи ($L = 84$ дБ): 26,7 % ($VBW = 30$ кГц); 19,9 % ($VBW = 10$ кГц) и 10,2% ($VBW = 3$ кГц);

Анализ результатов исследований, проведенных на 2-м этапе, показал, что:

разборчивость речи на выходе аналогового демодулятора существенно ниже, чем на выходе полосового фильтра. Очевидно, это обусловлено очень малой глубиной модуляции сигнала (от 0,2% – для 2-й октавной полосы, до 2,1% - для 6-й октавной полосы) и высоким уровнем шумов низкочастотного тракта;

максимальная разборчивость речи наблюдается при $VBW = 30$ кГц.

Таким образом, в ходе экспериментальных исследований установлено, что наибольшая разборчивость речи наблюдается при измерении уровней модуляционных составляющих высокочастотных сигналов, переизлученных ТС, на выходе полосового фильтра при $RBW = 10$ Гц. Следовательно, именно данный метод измерений целесообразно использовать при оценке возможностей технических средств разведки (ТСР) по перехвату речевой информации методом «высокочастотной накачки» технических средств, установленных в выделенном помещении.

Результаты расчета словесной разборчивости, полученные в ходе экспериментальных исследований, основываются на использовании в качестве приемного устройства анализатора спектра «Rohde&Schwarz FSL3» с измерительной антенны Пб-51, при ее установке на расстоянии 1 м от телефонного аппарата.

На частоте 230 МГц спектральная чувствительность антенны Пб-51 составляет $E_a \approx -29,6$ дБ(мкВ/√Гц), а значение коэффициента калибровки – $k_a \approx 18,1$ дБ(1/м). Шумы антенны, пересчитанные на вход приемного устройства, составляют $U_{ш.а} \approx -47,7$ дБ(мкВ/√Гц), что значительно выше собственных шумов приемного устройства $U_{ш.прм} \approx -56,6$ дБ(мкВ/√Гц). Однако, шумы антенны существенно ниже шумов, измеренных в ходе экспериментальных испытаний (таблица 3).

Таблица 3

Уровни шумов в октавных полосах

Номер октавной полосы (диапазон частот, Гц)	Результаты измерений уровня шума ($\Delta F=10$ Гц), $U_{ш}$, дБмкВ	Уровень шумов в октавных полосах	
		Рассчитанные по результатам измерений, $U_{ш}$, дБмкВ	Рассчитанные по характеристикам антенны, $U_{ш.а}$, дБмкВ
2 (180 – 355)	-17,38	-4,88	-25,20
3 (355 – 710)	-16,39	-1,55	-22,86
4 (710 – 1420)	-17,55	0,95	-19,19
5 (1420 – 2840)	-22,19	-0,66	-16,18
6 (2840 – 5680)	-21,63	2,90	-13,17

Следовательно, при оценке возможностей ТСП по перехвату речевой информации методом «высокочастотной накачки» технических средств, кроме шумов антенны и приемного устройства, необходимо учитывать шумы, создаваемые техническим средством, которые, при пересчете на вход приемного устройства значительно выше как шумов антенны, так и собственных шумов приемного устройства.

На расстоянии $r = 1$ м от ТС (телефонного аппарата) шумы на входе приемного устройства, обусловленные шумами ТС, существенно выше как собственных шумов приемного устройства, так и шумов антенны. Следовательно, для $r = 1$ м можно полагать, что $U_{ш.и} \approx U_{ш.тс.и}$.

С увеличением расстояния, вследствие затухания электромагнитных излучений (ЭМИ), будет падать как напряжение информативного сигнала на входе приемного устройства, так и напряжение шумов, обусловленных шумами ТС, но при этом напряжение шумов антенны, пересчитанное на вход приемного устройства, и напряжение собственных шумов приемного устройства будут оставаться неизменными.

Учитывая, что шумы антенны (Пб-51), пересчитанные на вход приемного устройства, значительно выше собственных шумов приемного устройства (FSL - 3), напряжение шумов на входе приемного устройства для i -й октавной полосы на расстоянии r от ТС можно рассчитать по формуле:

$$U_{ш.и.r} \approx 20 \lg \sqrt{10^{0,1 \cdot (U_{ш.тс.и} - V_r)} + 10^{0,1 \cdot (U_{ш.а.и})}}, \quad (4)$$

где $U_{ш.и.r}$ – напряжение шумов на входе приемного устройства для i -й октавной полосы на расстоянии r от ТС, дБ;

$U_{ш.а.и}$ – напряжение шумов антенны, пересчитанное на вход приемного устройства, для i -й октавной полосы, дБ;

$U_{ш.тс.и}$ – напряжение шумов на входе приемного устройства, обусловленных шумами технического средств (ТС), для i -й октавной полосы, измеренное на расстоянии $r = 1$ м от ТС, дБ.

V_r – затухание ЭМИ на частоте сигнала f на расстоянии r от ТС, дБ.

Учитывая, что измерение ЭМИ проводилось на расстоянии $r = 1$ м, для расчета затухания ЭМИ на расстоянии r от ТС воспользуемся формулой [3]:

$$V_r \approx 20 \lg \left(\frac{r^3}{\frac{k^4 r^4 - k^2 r^2 + 1}{k^4 - k^2 + 1}} \right), \quad (5)$$

где $k = \frac{2\pi}{\lambda} = \frac{2\pi \cdot f}{300}$ – волновое число;

λ – длина волны излучения, м;

f – частота излучения, МГц;

r – расстояние от источника излучения, м.

С учетом формул (4) и (5) отношение сигнал/шум на входе приемного устройства можно рассчитать по формуле:

$$q_{c.m.i.r} = U_{c.m.i} - V_r - U_{ш.i.r}. \quad (6)$$

где $q_{c.m.i.r}$ – отношение сигнал/шум для i -й октавной полосы, соответствующее уровню тестового акустического сигнала, рассчитанное для расстояния r , дБ.

В таблице 4 приведены результаты расчетов разборчивости речи при различных уровнях речи на различных расстояниях.

Таблица 4

Результаты расчетов разборчивости речи на различных расстояниях

Расстояние от ТС	Разборчивость речи (%) при типовом уровне речевого сигнала (L), дБ		
	$L=70$	$L=76$	$L=84$
$r = 1$ м	8,30	28,00	74,12
$r = 5$ м	6,09	22,04	65,32
$r = 10$ м	3,37	13,79	49,77
$r = 15$ м	1,85	8,54	36,89
$r = 20$ м	1,07	5,47	27,51
$r = 25$ м	0,65	3,64	20,84
$r = 30$ м	0,42	2,52	16,07
$r = 35$ м	0,28	1,79	12,60
$r = 40$ м	0,19	1,31	10,04
$r = 45$ м	0,14	0,99	8,11

Таким образом, анализ результатов проведенных исследований показал, что при использовании в качестве приемного устройства средства перехвата анализатора спектра FSL-3 с антенной П6-51:

словесная разборчивость речи на выходе аналогового демодулятора анализатора спектра при расположении антенны на удалении 1 м от телефонного аппарата не превышает 26,7% даже для очень громкой речи ($L = 84$ дБ). Очевидно, это обусловлено очень малой глубиной модуляции сигнала (менее 2%) и высоким уровнем шумов низкочастотного тракта;

отношения сигнал/шум для информативных (боковых) составляющих на выходе полосового фильтра анализатора спектра достаточны для обеспечения высокой разборчивости речи при использовании цифровых методов демодуляции сигналов;

при использовании цифровых методов демодуляции сигналов словесная разборчивость речи может составлять: для громкой речи более 22% на дальностях до 5 м; для очень громкой речи – более 20% на дальностях до 25 м.

Литератур

1. Хорев А.А., Чачилло Т. В. Исследование подверженности телефонного аппарата «высокочастотной накачке» // Вестник УрФО. Безопасность в информационной сфере. – 2025. – № 2(56). – С. 80-95.
2. Хорев А.А. Техническая защита информации: учеб. пособие: В 3-х т. Т. 1: Технические каналы утечки информации. -М.: НПЦ «Аналитика», 2008. – 436 с.
3. Хорев А.А., Борисов Р.М. Методика расчета затухания побочных электромагнитных излучений средств вычислительной техники// Всероссийская конференция «Радиоэлектронные устройства и системы для инфотелекоммуникационных технологий – РЭУС-2026». Доклады. – М.: РНТОРЭС имени А.С. Попова, 2026. – С. ISBN 978-5-905278-62-4

INVESTIGATION OF THE EFFECT OF THE RECEIVING DEVICE BANDWIDTH ON SPEECH INTELLIGIBILITY DURING THE INTERCEPTION OF INFORMATION BY THE "HIGH-FREQUENCY PUMPING" METHOD

Prof. Horev A.A., stud. T.V. Chachillo

National Research University of Electronic Technology

The article presents the results of experimental studies of the dependence of verbal intelligibility of speech on the bandwidth of the receiving device (RBW and VBW) when intercepting acoustic speech information using the "high-frequency pumping" method of a telephone device. The studies were conducted for RBW – 30 Hz and 10 Hz and VBW – 30 kHz, 10 kHz and 3 kHz. Experimental studies have shown that the verbal intelligibility of speech at the output of the analog demodulator of the spectrum analyzer when the antenna is located at a distance of 1 m from the telephone does not exceed 26,7%, even for very loud speech ($L = 84$ dB). When using digital signal demodulation methods, verbal intelligibility of speech can be: for loud speech, more than 22% at ranges up to 5 m; for very loud speech, more than 20% at ranges up to 25 m. At the same time, changing the RBW bandwidth does not significantly affect speech intelligibility.



АВТОРСКИЙ УКАЗАТЕЛЬ.

Аветисян Т.В.	47	Жукова А. А.	296	Пилюгин П.Л.	384, 389
Андриянов Н.А.	111	Жук А.П.	55	Попов М.Ю.	84
Антонов Д.И.	116	Ибрагимов Р.М.	181	Порхун А.С.	394
Артемов Д.Д.	127	Иванов А. И.	143	Преображенский А.П.	47
Бабенко М.Г.	402	Иванов А.В.	208	Преображенский Ю.П.	47
Баннх А. Г.	143	Иванов А.В.	300	Проворнов И. А.	399
Баранова Е.И.	249	Кальченко М.Д.	304	Радаев О.А.	62
Баскаков А.Е.	52	Кандидатов Р.А.	379	Реджепов И.В.	84
Белов А.А.	121	Карасев Н.А.	309	Русанов М.А.	167
Белоконь Д.А.	212	Квашенников В.В.	67	Рябов Д.А.	178
Борисов Р.М.	228, 234	Кеньков Е. А.	332	Саакян Э.А.	90
Браже Р.А.	159	Кокутин С.Н.	148	Санамян О.А.	154
Брусенцов К.А.	58, 218	Кононов В.О.	314	Селюшкин М.А.	171
Букинин П.А.	239	Королев А.В.	42	Семенов Г.А.	154
Буренок Д.С.	244	Кочедыков С.С.	319, 411	Сергеев В.А.	62
Буров Ю.Я.	95	Кривальцевич С.В.	38	Сергиев С.А.	148
Бурова А.Ю.	95	Кузнецов А.М.	326	Синицын А.А.	402
Бутакова Н.Г.	249, 271, 415	Кузьмин Н.П.	62	Слободсков О.Е.	84
Быков А.И.	254	Кутузов В. М.	18	Смирнов А.С.	406
Винник Е.А.	249	Лапина М. А.	154, 167, 332	Сотникова Н.В.	58, 218
Виноградов И.В.	258	Лебедев Е.Ю.	159	Страхов С.Ю.	58, 218
Витязев С.В.	127	Линец Г.И.	9	Татарчук М.Д.	411
Воеводин В.А.	258	Лукманова О.Р.	337	Ташев Н.С.	35
Волошин Е.А.	193	Львов К.А.	342	Ташлинский А.Г.	121, 181
Габеркорн А.Э.	263	Лэ В.Т.	14	Тоискин В.Е.	72, 101
Гапочкин А.В.	189	Май Т. З.	18	Томчук Д.Э.	415
Гончаров В.Д.	9	Малыгина Е. А.	143	Ушаков И.А.	420
Гринев Е. М.	200	Марков А.С.	28	Филимонова С.Р.	300
Дасибинба У.	275	Маругин А. С.	31	Филипов И. А.	143
Девятяров В.Б.	84	Марченков М.О.	163	Филиппова П.В.	249
Деменский Д. С.	79	Мельников С.В.	9	Фролов И.В.	62
Денисов В.Д.	284	Минкин А.Д.	347	Хорев А.А.	228, 234, 352
Джиган В.И.	6	Мокринский Д.В.	72, 101		357, 424, 430
Диптан П.А.	200, 223	Моложавцев Е.О.	352, 357	Чачилло Т.В.	430
Дмитриев И.А.	280	Нгуен Д.В.	14	Шабанов А.К.	67
Дорогов А.Ю.	132, 137	Нгуен Тхань Хынг	23	Шагарова Л.В.	38
Душкин А.В.	284, 342, 370	Ненашева Ю.А.	394	Шкилевич Н.Н.	293
Душкин А.В.	288	Николаев Р.С.	366	Шумилов Н.Н.	107
Дюков А.В.	47	Нилов Н.А.	370	Щербаков В.А.	171, 288,
Ерасов А.Б.	411	Облиенко А.В.	254, 284		374, 406
Ермакова А. И.	143	Орехов С. Е.	79	Юрченков В.О.	271
Ерохин С.Д.	384	Орлов В.К.	31	Яровой А.А.	186
		Орлов П.А.	374	Яшин В.А.	267
		Павлов С.Ю.	47	Яценко А.С.	8
		Панцыр Р.Я.	379		
		Парфенов А.А.	379		
		Пашинцев В.П.	200, 212		
		Петухов А.Н.	362, 384, 389		

Всероссийская конференция
РАДИОЭЛЕКТРОННЫЕ УСТРОЙСТВА И СИСТЕМЫ ДЛЯ
ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Д О К Л А Д Ы

Серия: научные конференции, посвящённые Дню Радио

Выпуск: LXXXI

107031, Москва, К-31, ул. Рождественка, д.:6/9/20, стр.1

Рабочая группа от РНТОРЭС им. А.С. Попова

Телефоны:		E-mail:
Сотовый: +7(903)201-53-33	 Организационные вопросы. Самсонов Геннадий Андреевич Ответственный организатор конференции от РНТОРЭС им. А.С. Попова	rntores@mail.ru
Сотовый: +7(925)585-80-84	 Приём докладов. Третьяков Геннадий Николаевич Главный учёный секретарь РНТОРЭС им А.С. Попова	doklad-rntores@mail.ru
Сотовый: +7(985)733-91-91	 Зав. Организац-контрольным отделом Карпушкина Галина Ивановна Распространение Сборников докладов РНТОРЭС им. А.С. Попова	vznos-rntores@mail.ru

Сайт РНТОРЭС им. А.С. Попова: <http://www.rntores.ru/>