Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.

ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ НЕКВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
31.08.2026
Владелец: к.т.н. Рева И. Л.
Срок действия: не ограничен
Адрес хранения электронного документа:
https://www.nstu.ru/university/info/sveden/education

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методология безопасной разработки и эксплуатации программного обеспечения

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Безопасность значимых объектов критической информационной инфраструктуры

Курс: 4, семестр : 8

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**8**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	48
4	Лекции, час.	18
5	Практические занятия, час.	18
6	Лабораторные занятия, час.	0
7	из них в активной и интерактивной форме, час.	0
8	из них практической подготовки, час.	18
9	Аттестация, час.	2
10	Консультации, час.	10
11	Самостоятельная работа, час.	60
12	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ(Р)/реферат, подготовка к контрольной работе)	
13	Вид аттестации	3

Новосибирск 2026

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС введен в действие приказом №1457 от 26.11.2020 г. , дата утверждения: 17.02.2021 г.

Место дисциплины в структуре учебного плана: Блок 1, обязательная

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

Рабочая программа обсуждена на заседании кафедры

ЗИ, 31.08.2026

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 8 от 31.08.2026

Заведующий кафедрой:

доцент, к.т.н. Иванов А. В.

Ответственный за образовательную программу:

заведующий кафедрой Иванов А. В.

1. Внешние требования

Таблица 1.1

Группа	Компетенции
	Индикаторы достижения компетенций
Общепрофессиональные компетенции	ОПК-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем
	ОПК-11. 1 Владеет навыками разработки компонентов систем защиты информации автоматизированных систем
	ОПК-11. 2 Умеет применять методы разработки компонентов систем защиты информации автоматизированных систем
Общепрофессиональные компетенции	ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности
	ОПК-2. 1 Знает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства
	ОПК-2. 2 Умеет применять современные информационно-коммуникационные технологии и программные средства для решения задач профессиональной деятельности с соблюдением норм информационной безопасности

2. Требования НГТУ к планируемым результатам обучения, соотнесенным с индикаторами достижения компетенций

Таблица 2.1

Индикаторы достижения компетенций Результаты обучения	Формы организации занятий
ОПК-11. 1 Владеет навыками разработки компонентов систем защиты информации автоматизированных систем	
Имеет опыт применения основных программных средств контроля защищенности автоматизированных систем	Лекции; Практические занятия; Самостоятельная работа
ОПК-11. 2 Умеет применять методы разработки компонентов систем защиты информации автоматизированных систем	
Имеет опыт проведения оценки рисков информационной безопасности	Лекции; Практические занятия; Самостоятельная работа
ОПК-2. 1 Знает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства	
Знает как использовать программные средства анализа и управления рисками	Лекции; Практические занятия; Самостоятельная работа
Имеет представление о требованиях к автоматизированным системам в защищенном исполнении	Лекции; Практические занятия; Самостоятельная работа
ОПК-2. 2 Умеет применять современные информационно-коммуникационные технологии и программные средства для решения задач профессиональной деятельности с соблюдением норм информационной безопасности	
Умеет применять языки, системы и инструментальные средства программирования в профессиональной деятельности	Лекции; Практические занятия; Самостоятельная работа

3. Содержание и структура дисциплины

Таблица 3.1

Темы лекций	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций
Семестр: 8				

Дидактическая единица: Аудит информационной безопасности и понятие тестирование на проникновение				
1. Основные методы и подходы аудита информационной безопасности и приложений.	2	0	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2
Дидактическая единица: Безопасность web-приложений				
2. Основные уязвимости и понятия, которые встречаются при реализации web-приложений	2	0	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2
3. Внедрение кода на клиенте. CSRF-атаки. Инструментарий для анализа web-приложений	2	0	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2
4. Внедрение кода на сервере.	4	0	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2
Дидактическая единица: Программные уязвимости				
5. Уязвимости, связанные с манипуляциями программной памяти	2	0	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2
6. Ошибки, связанные с целочисленным программированием	2	0	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2
7. Изучение программных средств анализа кода	4	0	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2

Темы практических занятий	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций	Учебная деятельность
Семестр: 8					
Дидактическая единица: Аудит информационной безопасности и понятие тестирование на проникновение					
2. Подходы к поиску уязвимостей в ПО	4	4	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2	Изучение основных подходов к поиску уязвимостей в ПО
4. Уязвимости, связанные с политикой безопасности и бизнес-процессами организации. Социальная инженерия	6	6	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2	Уязвимости, связанные с политикой безопасности и бизнес-процессами организации. Социальная инженерия
Дидактическая единица: Безопасность web-приложений					
3. Обход аутентификации	4	4	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2	Обход аутентификации
Дидактическая единица: Программные уязвимости					

1. Раскрытие информации. Состояние гонки. Некорректная обработка исключений. Слабости в реализации криптографических модулей	4	4	0	ОПК-11.1,ОПК-11.2,ОПК-2.1,ОПК-2.2	Раскрытие информации. Состояние гонки. Некорректная обработка исключений. Слабости в реализации криптографических модулей

3.1 Практическая подготовка

Таблица 3.2

№	Темы занятий	Формы организации занятий	Содержание практической подготовки (виды работ)
1	Подходы к поиску уязвимостей в ПО	Пр	Выполняет следующие виды работ: выполняет практическую работу; оформляет отчет; защищает практическую работу
2	Уязвимости, связанные с политикой безопасности и бизнес-процессами организации. Социальная инженерия	Пр	Выполняет следующие виды работ: выполняет практическую работу; оформляет отчет; защищает практическую работу
3	Обход аутентификации	Пр	Выполняет следующие виды работ: выполняет практическую работу; оформляет отчет; защищает практическую работу
4	Раскрытие информации. Состояние гонки. Некорректная обработка исключений. Слабости в реализации криптографических модулей	Пр	Выполняет следующие виды работ: выполняет практическую работу; оформляет отчет; защищает практическую работу

3.2 Самостоятельная работа обучающегося

Таблица 3.3

№	Виды самостоятельной работы	Индикаторы достижения компетенций	Часы на выполнение	Часы на консультации
Семестр: 8				
1	Подготовка к занятиям	ОПК-11.1,ОПК-11.2,ОПК-2.1, ОПК-2.2	10	0
: Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 29.06.2022). – Режим доступа: по подписке.				
2	Дополнительная учебная деятельность	ОПК-11.1,ОПК-11.2,ОПК-2.1, ОПК-2.2	10	0
: Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 29.06.2022). – Режим доступа: по подписке.				
3	Подготовка к аттестации	ОПК-11.1,ОПК-11.2,ОПК-2.1, ОПК-2.2	40	10

: Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 29.06.2022). – Режим доступа: по подписке.

3.3 Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 3.4).

Таблица 3.4

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Среда электронного обучения НГТУ
Консультирование	e-mail; Среда электронного обучения НГТУ
Контроль	Среда электронного обучения НГТУ
Размещение учебных материалов	Среда электронного обучения НГТУ

4. Правила аттестации обучающихся по дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 4.1.

Таблица 4.1

Оцениваемые виды деятельности обучающихся	Мин. балл	Максимальный балл
Семестр: 8		
Практические занятия:	40	80
Зачет:	10	20

В таблице 4.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 4.2

Коды компетенций	Индикаторы достижения компетенций	Формы контроля	
			Зачет
ОПК-11	ОПК-11 1. Владеет навыками разработки компонентов систем защиты информации автоматизированных систем		+
	ОПК-11 2. Умеет применять методы разработки компонентов систем защиты информации автоматизированных систем		+
ОПК-2	ОПК-2 1. Знает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства		+
	ОПК-2 2. Умеет применять современные информационно-коммуникационные технологии и программные средства для решения задач профессиональной деятельности с соблюдением норм информационной безопасности		+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

5. Литература

Основная литература

1. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. - 198 с.: ISBN 978-5-4446-1043-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/977192 (дата обращения: 29.06.2022). – Режим доступа: по подписке.

2. Гагарина, Л. Г. Технология разработки программного обеспечения : учебное пособие / Л.Г. Гагарина, Е.В. Кокорева, Б.Д. Сидорова-Виснадул ; под ред. Л.Г. Гагариной. — Москва : ИНФРА-М, 2026. — 400 с. — (Среднее профессиональное образование). - Текст : электронный. - URL: https://znanium.ru/catalog/product/2212387 (дата обращения: 09.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=467899 - Загл. с экрана.

Дополнительная литература

1. Аппаратные и программные средства защиты информации: Учебное пособие / Душкин А.В., Кольцов А., Кравченко А. - Воронеж:Научная книга, 2016. - 232 с. ISBN 978-5-4446-0746-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/923168 (дата обращения: 29.06.2022). – Режим доступа: по подписке.

2. Поддержка принятия решений при проектировании систем защиты информации : монография / В.В. Бухтояров, М.Н. Жукова, В.В. Золотарев [и др.]. — Москва : ИНФРА-М, 2020. — 131 с. — (Научная мысль). — www.dx.doi.org/10.12737/2248. - ISBN 978-5-16-009519-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1036519 (дата обращения: 29.06.2022). – Режим доступа: по подписке.

Интернет-ресурсы

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Саратов : Профобразование, 2017.— 702 с. — Режим доступа : http://www.iprbookshop.ru/63594.html. — Загл. с экрана.

6. Методическое и программное обеспечение, информационные технологии

6.1 Методическое обеспечение

1. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 29.06.2022). – Режим доступа: по подписке.

6.2 Специализированное программное обеспечение

1 Офисный пакет приложений Microsoft Office

2 ОС для применения на серверах Microsoft Windows

6.3 Информационные технологии

При осуществлении образовательного процесса по дисциплине применяются элементы дистанционных образовательных технологий, а также синхронного и асинхронного взаимодействия в электронной информационно-образовательной среды НГТУ.

7. Материально-техническое обеспечение

Компьютерный класс

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Оборудование для проведения лекционных и практических занятий
2	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Проведение практических занятий