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
Методы и средства криптографической защиты информации

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

Курс: 3, семестр : 5

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**5**
1	Всего зачетных единиц (кредитов)	4
2	Всего часов	144
3	Всего занятий в контактной форме, час.	68
4	Лекции, час.	36
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	8
8	из них практической подготовки, час.	8
9	Аттестация, час.	2
10	Консультации, час.	12
11	Самостоятельная работа, час.	76
12	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ(Р)/реферат, подготовка к контрольной работе)	Р
13	Вид аттестации	Э

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-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности
	ОПК-10. 1 Владеет методами и средствами криптографической и технической защиты информации
	ОПК-10. 2 Умеет пользоваться нормативными документами в области технической защиты информации, применения методов криптографической защиты, анализировать и оценивать угрозы информационной безопасности объекта информатизации
	ОПК-10. 3 Знает основные понятия и задачи криптографии, математические модели криптографических систем

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

Таблица 2.1

Индикаторы достижения компетенций	Формы организации занятий
Результаты обучения	
ОПК-10. 1 Владеет методами и средствами криптографической и технической защиты информации	
Умеет применять требования по криптографической защите информационных систем	Лекции; Лабораторные работы; Самостоятельная работа
ОПК-10. 2 Умеет пользоваться нормативными документами в области технической защиты информации, применения методов криптографической защиты, анализировать и оценивать угрозы информационной безопасности объекта информатизации	
Имеет опыт применения математических моделей в криптографии	Лекции; Лабораторные работы; Самостоятельная работа
ОПК-10. 3 Знает основные понятия и задачи криптографии, математические модели криптографических систем	
Знает как решать задачи криптографии	Лекции; Лабораторные работы; 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: 5				
Дидактическая единица: Основные характеристики шифров				
1. Модели шифров	6	0	0	ОПК-10.1,ОПК-10.2,ОПК-10.3
2. Стойкости шифров	6	0	0	ОПК-10.1,ОПК-10.2,ОПК-10.3
Дидактическая единица: Симметричная криптография				
3. Блочные и потоковые шифры	6	0	0	ОПК-10.1,ОПК-10.2,ОПК-10.3

4. Генераторы псевдослучайных последовательностей	6	0	0	ОПК-10.1,ОПК-10.2,ОПК-10.3
Дидактическая единица: Ассиметричная криптография				
5. Принципы построения криптосистем с открытым ключом	6	0	0	ОПК-10.1,ОПК-10.2,ОПК-10.3
6. Особенности системы	6	0	0	ОПК-10.1,ОПК-10.2,ОПК-10.3

Темы лабораторных работ	Часы	Из них в форме практ. подг., час.	Активные формы, час.	Индикаторы достижения компетенций	Учебная деятельность
Семестр: 5					
Дидактическая единица: Основные характеристики шифров					
1. Оценка стойкости различных шифров	6	4	4	ОПК-10.1,ОПК-10.2,ОПК-10.3	Оценка стойкости и программная реализация шифров
Дидактическая единица: Симметричная криптография					
2. Сравнительный анализ симметричных шифров	6	2	2	ОПК-10.1,ОПК-10.2,ОПК-10.3	Сравнительный анализ симметричных шифров
Дидактическая единица: Ассиметричная криптография					
3. Сравнительный анализ ассиметричных шифров	6	2	2	ОПК-10.1,ОПК-10.2,ОПК-10.3	Сравнительный анализ ассиметричных шифров

3.1 Практическая подготовка

Таблица 3.2

№	Темы занятий	Формы организации занятий	Содержание практической подготовки (виды работ)
1	Оценка стойкости различных шифров	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
2	Сравнительный анализ симметричных шифров	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу
3	Сравнительный анализ ассиметричных шифров	Лб	Выполняет следующие виды работ: выполняет лабораторную работу; оформляет отчет; защищает лабораторную работу

3.2 Самостоятельная работа обучающегося

Таблица 3.3

№	Виды самостоятельной работы	Индикаторы достижения компетенций	Часы на выполнение	Часы на консультации
Семестр: 5				
1	РГЗ/Реферат	ОПК-10.1,ОПК-10.2,ОПК-10.3	26	6

: Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2016.- 57, [1] с.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326 Котов Ю. А. Приложения шифров. Криптоанализ : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2019.- 74, [2] с. : схемы, табл.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000241161				
2	Подготовка к занятиям	ОПК-10.1,ОПК-10.2	12	0
: Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2016.- 57, [1] с.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326				
3	Дополнительная учебная деятельность	ОПК-10.3	12	0
: Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2016.- 57, [1] с.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326				
4	Подготовка к аттестации	ОПК-10.1,ОПК-10.2,ОПК-10.3	26	6
: Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2016.- 57, [1] с.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326 Котов Ю. А. Приложения шифров. Криптоанализ : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2019.- 74, [2] с. : схемы, табл.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000241161				

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: 5		
Лабораторная:	15	30
РГЗ/Реферат:	15	30
Экзамен:	20	40

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

Таблица 4.2

Коды компетенций	Индикаторы достижения компетенций	Формы контроля	
		Защита РГЗ/Р	Экзамен
ОПК-10	ОПК-10 1. Владеет методами и средствами криптографической и технической защиты информации	+	+
	ОПК-10 2. Умеет пользоваться нормативными документами в области технической защиты информации, применения методов криптографической защиты, анализировать и оценивать угрозы информационной безопасности объекта информатизации	+	+
	ОПК-10 3. Знает основные понятия и задачи криптографии, математические модели криптографических систем	+	+

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

5. Литература

Основная литература

1. Котов Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : [учебное пособие] / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2017.- 64, [2] с. : ил., табл.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000236930

2. Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2026. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2241407 (дата обращения: 09.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=478947 - Загл. с экрана.

Дополнительная литература

1. Введение в информационную безопасность и защиту информации : [учебное пособие / В. А. Трушин и др.] ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2017.- 130, [2] с. : ил. табл.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235435

2. Методы и средства комплексной защиты информации в технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. - Саров : РФЯЦ-ВНИИЭФ, 2019. - 224 с. - ISBN 978-5-9515-0429-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1230827 (дата обращения: 09.07.2026). – Режим доступа: по подписке. - Режим доступа: https://znanium.ru/catalog/document?id=370734 - Загл. с экрана.

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. Котов Ю. А. Приложения шифров. Криптоанализ : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2019.- 74, [2] с. : схемы, табл.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000241161

2. Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т.- Новосибирск: Изд-во НГТУ, 2016.- 57, [1] с.- Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326

6.2 Специализированное программное обеспечение

1 Пакет офисных 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

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Оборудование используется при изучении тематического плана дисциплины

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Для проведения практических и лабораторных занятий