

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Анатольевна

Должность: и.о. декана факультета математики и компьютерных наук имени
профессора Н.И. Червякова

Дата подписания: 19.06.2026 15:33:13

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

И.о. декана факультета
математики и компьютерных
наук имени профессора Н.И. Червякова
Грובה Т.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методы и средства криптографической защиты информации»

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	6

Разработано

Лапина М.А. - доцент кафедры
вычислительной математики и
кибернетики.

Ставрополь 2026 г.

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Методы и средства криптографической защиты информации» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем фундаментальных знаний и практических навыков в области криптографических методов защиты информации, включая современные алгоритмы шифрования, электронную подпись, хеширование и управление криптографическими ключами.

Задачи дисциплины:

- изучение теоретических основ криптографии, включая симметричные и асимметричные алгоритмы шифрования;
- освоение принципов построения и применения криптографических протоколов;
- формирование навыков анализа стойкости криптографических алгоритмов;
- изучение методов генерации, распределения и хранения криптографических ключей;
- приобретение практических умений реализации криптографических механизмов защиты информации;
- освоение стандартов и нормативных требований к криптографической защите данных;
- развитие компетенций в области криптоанализа и оценки защищенности криптосистем.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и средства криптографической защиты информации» относится к части, формируемой участниками образовательных отношений дисциплинам (модулям) обязательной части. Ее освоение происходит в 6 семестре.

3. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ИД-1ОПК-10 Понимает базовые принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности.	Предоставляет детальный отчет с полным пояснением, где использует основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности.
	ИД-2ОПК-10 Использует средства криптографической и технической защиты информации для решения задач профессиональной деятельности.	Предоставляет детальный отчет с полным пояснением, в котором показывает способность использовать средства криптографической и технической защиты информации для решения задач профессиональной деятельности
	ИД-3ОПК-10 Выбирает оптимальный вариант использования навыков и методик	Предоставляет детальный отчет, в котором показывает своё умение пользоваться и применять навыки и

	применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	методики применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности
--	--	---

4. Объем учебной дисциплины и формы контроля *

Объем занятий: всего: 5 з.е. 180 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	48/2
Лабораторных работ/из них практическая подготовка	48/0
Практических занятий/из них практическая подготовка	0
Самостоятельная работа	48
Формы контроля	
Экзамен 6 семестр	36
Зачет	-
Зачет с оценкой	-
Курсовая работа	нет

* Дисциплина предусматривает применение электронного обучения, дистанционных образовательных технологий

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества часов и видов занятий

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	очная форма				Формы текущего контроля успеваемости и
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов	
			Лекции	Практические занятия	Лабораторные работы		
	6 СЕМЕСТР						
1.	Методы криптографического преобразования информации Изучение основных подходов к защите данных с помощью шифрования. В данной теме студентам предстоит изучить основные методы криптографического преобразования информации, включая симметричное и асимметричное шифрование. Особое внимание будет уделено принципам безопасности и областям применения. В конце изучения темы студент будет понимать, как и когда применяются криптографические методы защиты данных.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование

2.	Шифрование информации Практика применения симметричных и асимметричных алгоритмов шифрования. В данной теме студентам предстоит на практике применять алгоритмы симметричного (например, AES) и асимметричного (например, RSA) шифрования. Особое внимание будет уделено ключевому управлению, шифрованию и расшифровке. В конце изучения темы студент будет уметь реализовывать базовые операции шифрования.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4/2	-	4	4	Собеседование
3.	Стеганография Скрытие информации в изображениях, аудио и других форматах. В данной теме студентам предстоит изучить основы стеганографии — скрытия информации внутри других типов файлов, таких как изображения или аудиофайлы. Особое внимание будет уделено методам внедрения и извлечения данных. В конце изучения темы студент будет знать способы скрытого обмена информацией.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование
4.	Кодирование информации Разбор кодов для повышения надёжности передачи данных. В данной теме студентам предстоит изучить методы кодирования информации для повышения надёжности передачи данных. Особое внимание будет уделено избыточному и коррекционному кодированию. В конце изучения темы студент будет уметь использовать базовые коды (например, Хэмминга) для контроля ошибок.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование
5.	Сжатие информации Анализ алгоритмов сжатия без потерь и с потерями. В данной теме студентам предстоит исследовать алгоритмы сжатия информации, как без потерь (например, Huffman), так и с потерями (например, JPEG). Особое внимание будет уделено оценке эффективности и применению. В конце изучения темы студент будет понимать различие и выбор метода сжатия по задачам.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование

6.	Традиционные методы шифрования Изучение исторических шифров: Цезаря, Виженера и др. В данной теме студентам предстоит познакомиться с традиционными методами шифрования, включая шифр Цезаря, шифр Виженера и другие исторические системы. Особое внимание будет уделено их алгоритмическому устройству и уязвимостям. В конце изучения темы студент будет понимать эволюцию шифров.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование
7.	Методы криптографического преобразования информации Практика применения различных криптографических методов в ИБ. В данной теме студентам предстоит на практике применить различные криптографические методы в задачах информационной безопасности. Особое внимание будет уделено выбору метода под конкретную задачу и реализации базовых схем защиты. В конце изучения темы студент будет уметь проектировать простые схемы защиты.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование
8.	Электронная цифровая подпись Применение ЭЦП для обеспечения целостности и подлинности данных. В данной теме студентам предстоит изучить принципы работы электронной цифровой подписи (ЭЦП). Особое внимание будет уделено обеспечению целостности и подлинности данных с помощью ЭЦП. В конце изучения темы студент будет знать, как устроена и применяется ЭЦП в юридически значимых документах.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование
9.	Криптоанализ и методы взлома шифров Анализ уязвимостей алгоритмов, методы перебора и атаки. В данной теме студентам предстоит изучить методы криптоанализа — взлома шифров. Особое внимание будет уделено подбору ключей, атакам на основе известных текстов и уязвимостям алгоритмов. В конце изучения темы студент будет уметь анализировать стойкость шифров.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование

10.	Хеширование и защита паролей Работа с хеш-функциями и методами безопасного хранения паролей. В данной теме студентам предстоит изучить принципы хеширования и способы защиты паролей. Особое внимание будет уделено однонаправленным хеш-функциям, соли и процедурам безопасного хранения. В конце изучения темы студент будет уметь проектировать безопасную систему хранения аутентификационных данных.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование
11.	Современные алгоритмы шифрования (AES, RSA) Применение и сравнение ключевых стандартов современной криптографии. В данной теме студентам предстоит познакомиться с современными алгоритмами шифрования, такими как AES и RSA. Особое внимание будет уделено отличиям между ними, устойчивости и применению. В конце изучения темы студент будет уметь выбирать и применять соответствующий алгоритм по контексту задачи.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование
12.	Квантовая криптография Введение в основы квантовой защиты информации и передачи ключей. анной теме студентам предстоит получить вводные знания о квантовой криптографии. Особое внимание будет уделено квантовой передаче ключей, принципу неопределённости и защите от перехвата. В конце изучения темы студент будет понимать перспективы и ограничения квантовой ИБ.	ОПК-10 ИД-1ОПК-10 ИД-2ОПК-10 ИД-3ОПК-10	4	-	4	4	Собеседование
	ИТОГО за 6 семестр		48/2	-	48	48	
	ИТОГО		48/2	-	48	48	

6. Фонд оценочных средств по дисциплине

Фонд оценочных средств (ФОС) по дисциплине базируется на перечне осваиваемых компетенций с указанием индикаторов. ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций (включаются в методические указания по тем видам работ, которые предусмотрены учебным планом и предусматривают оценку сформированности компетенций);
- типовые оценочные средства, необходимые для оценки знаний, умений и уровня сформированности компетенций.

ФОС является приложением к данной программе дисциплины.

7. Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина «Методы и средства криптографической защиты информации» построена по тематическому принципу, каждая тема представляет собой логически завершённый раздел.

Теоретический материал посвящён рассмотрению ключевых, базовых положений курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Лабораторные работы направлены на приобретение опыта практической работы в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим и лабораторным занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины, необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

8.1.1. Перечень основной литературы:

1. Бутакова, Н. Г. Криптографические методы и средства защиты информации : учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург : Интермедия, 2020. — 380 с. — ISBN 978-5-4383-0210-0
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии : учебное пособие, 3-е изд., испр. и доп. М. : Гелиос АРВ, 2005. 480 с.
3. Гашков С.Б., Применко М.А., Черепнев М.А. Криптографические методы защиты информации. М. : Изд. Центр «Академия», 2010.

8.1.2. Перечень дополнительной литературы:

1. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. М. : Науч. Мир, 2004.
2. Сингх С. Книга шифров: тайная история шифров и их расшифровки. М.: АСТ: Астрель, 2007.

8.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Методы и средства криптографической защиты информации». Ставрополь : СКФУ, 2026.
2. Методические указания к практическим занятиям по дисциплине «Методы и средства криптографической защиты информации». Ставрополь : СКФУ, 2026.

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://el.ncfu.ru/> – система управления обучением ФГАОУ ВО СКФУ.
Дистанционная поддержка дисциплины «Методы и средства криптографической защиты информации»
2. <http://www.un.org> - Сайт ООН Информационно-коммуникационные технологии
3. <http://www.intuit.ru> – Интернет-Университет Компьютерных технологий.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На практических занятиях студенты защищают отчеты по работам, которые они выполняют самостоятельно или в команде с применением компьютерной техники и Интернет-технологий

Информационные справочные системы:

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1	https://www.garant.ru/
2	http://www.consultant.ru/

Программное обеспечение:

1.	Альт Рабочая станция 10
2.	Альт Рабочая станция К
3.	Альт «Сервер»
4.	Пакет офисных программ - Р7-Офис

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.
Лабораторные занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.
Самостоятельная работа	Помещение для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и возможностью доступа к электронной информационно-образовательной среде университета

11. Особенности освоения дисциплины лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины обеспечивается:

- 1) для лиц с ограниченными возможностями здоровья по зрению:
 - присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе, записывая под диктовку),
 - письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,
 - специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
 - индивидуальное равномерное освещение не менее 300 люкс,
 - при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;
- 2) для лиц с ограниченными возможностями здоровья по слуху:
 - присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе, записывая под диктовку),
 - обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;
 - обеспечивается надлежащими звуковыми средствами воспроизведения информации;
- 3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):
 - письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
 - по желанию студента задания могут выполняться в устной форме.

12. Особенности реализации дисциплины с применением дистанционных образовательных технологий и электронного обучения

Согласно части 1 статьи 16 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» под *электронным обучением* понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. Под *дистанционными образовательными технологиями* понимаются образовательные технологии, реализуемые в основном с применением информационно-

телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Реализация дисциплины может быть осуществлена с применением дистанционных образовательных технологий и электронного обучения полностью или частично. Компоненты УМК дисциплины (рабочая программа дисциплины, оценочные и методические материалы, формы аттестации), реализуемой с применением дистанционных образовательных технологий и электронного обучения, содержат указание на их использование.

При организации образовательной деятельности с применением дистанционных образовательных технологий и электронного обучения могут предусматриваться асинхронный и синхронный способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет».

При применении дистанционных образовательных технологий и электронного обучения в расписании по дисциплине указываются:

способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет» (ВКС-видеоконференцсвязь, ЭТ – электронное тестирование);

ссылки на электронную информационно-образовательную среду СКФУ, на образовательные платформы и ресурсы иных организаций, к которым предоставляется открытый доступ через информационно-телекоммуникационную сеть «Интернет»;

для синхронного обучения - время проведения онлайн-занятий и преподаватели;

для асинхронного обучения - авторы онлайн-курсов.

При организации промежуточной аттестации с применением дистанционных образовательных технологий и электронного обучения используются Методические рекомендации по применению технических средств, обеспечивающих объективность результатов при проведении промежуточной и государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры с применением дистанционных образовательных технологий (Письмо Минобрнауки России от 07.12.2020 г. № МН-19/1573-АН "О направлении методических рекомендаций").

Реализация дисциплины с применением электронного обучения и дистанционных образовательных технологий осуществляется с использованием электронной информационно-образовательной среды СКФУ, к которой обеспечен доступ обучающихся через информационно-телекоммуникационную сеть «Интернет», или с использованием ресурсов иных организаций, в том числе платформ, предоставляющих сервисы для проведения видеоконференций, онлайн-встреч и дистанционного обучения (МТС-Линк), а также с использованием возможностей социальных сетей для осуществления коммуникации обучающихся и преподавателей.

Учебно-методическое обеспечение дисциплины, реализуемой с применением электронного обучения и дистанционных образовательных технологий, включает представленные в электронном виде рабочую программу, учебно-методические пособия или курс лекций, методические указания к выполнению различных видов учебной деятельности обучающихся, предусмотренных дисциплиной, и прочие учебно-методические материалы, размещенные в информационно-образовательной среде СКФУ.