

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 15:45:29

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

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

УТВЕРЖДАЮ

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптографические протоколы

Специальность	10.05.01 Компьютерная безопасность
Специализация	Информационно-аналитическая и техническая экспертиза компьютерных систем
Форма обучения	очная
Год начала обучения	2026
Реализуется в семестре	7

Разработано:

Петросян Светлана Мартиковна,
старший преподаватель кафедры
вычислительной математики и
кибернетики

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины

Целью изучения дисциплины «Криптографические протоколы» является формирование набора общепрофессиональных компетенций студента специальности 10.05.01 Компьютерная безопасность специализации «Информационно-аналитическая и техническая экспертиза компьютерных систем».

Задачами освоения дисциплины «Криптографические протоколы» являются:

- приобретение знаний о назначении, принципах реализации и использования криптографических протоколов;
- формирование навыков анализа криптографических протоколов, программной реализации криптографических протоколов для решения задач защиты информации.

2. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина относится к дисциплинам обязательной части программы специалитета. Ее освоение происходит в 7 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 (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ИД-2 _{ОПК-10} конфигурирует средства криптографической защиты информации	Способен применять знания о криптографических протоколах для организации защищенного хранения информации и защищенного информационного обмена

4. Объем учебной дисциплины и формы контроля *

Объем занятий: всего: 4 з.е. 144 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	36
Лабораторных работ/из них практическая подготовка	
Практических занятий/из них практическая подготовка	36
Самостоятельная работа	72
Формы контроля	
Экзамен	
Зачет	
Зачет с оценкой	+

* Дисциплина предусматривает применение электронного обучения, дистанционных образовательных технологий (если иное не установлено образовательным стандартом)

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
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов	
			Лекции	Практические занятия	Лабораторные работы		
1	Тема № 1. Решение задач по формальному описанию криптографических протоколов Практическая работа № 2. Определение уязвимостей протоколов. Практическая работа № 3. Составление формального описания базовых криптографических протоколов.	ОПК-10 ИД-2 _{ОПК-10}	6	6		12	собеседование
2	Практическая работа № 4. Совершения обмена открытыми ключами Практическая работа № 5. Проверка чисел на простоту Практическая работа №6 Изучение хэш-функций семейств SHA, MD и хэш-функции ГОСТ	ОПК-10 ИД-2 _{ОПК-10}	4	4		8	собеседование
3	Практическая работа № 7 Решение задач по разделению секрета Практическая работа № 8 Использование криптографических примитивов в контексте криптографических протоколов Практическая работа № 9 Изучение протоколов аутентификации	ОПК-10 ИД-2 _{ОПК-10}	6	6		12	собеседование
4	Практическая работа № 10 Изучение протоколов односторонней аутентификации Практическая работа № 11 Изучение протоколов двусторонней аутентификации Практическая работа № 12 Изучение протоколов электронной подписи	ОПК-10 ИД-2 _{ОПК-10}	6	6		12	собеседование
5	Практическая работа № 13 Сравнение протоколов ЭП DSA и ГОСТ Практическая работа № 14 Изучение схем стираемой электронной подписи Практическая работа № 15 Формальное описание протоколов слепой, совместной и подтверждаемой ЭП	ОПК-10 ИД-2 _{ОПК-10}	8	8		16	собеседование

6	Практическая работа № 16 Изучение и формальное описание протоколов голосования Практическая работа № 17 Изучение программных средств, реализующих протоколы электронной коммерции Практическая работа № 18 Решение задач по теме «Протоколы разделения секрета»	ОПК-10 ИД-2 _{ОПК-10}	6	6		12	собеседование
	ИТОГО за 7 семестр		36	36		72	

6. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю) базируется на перечне осваиваемых компетенций с указанием этапов их формирования в процессе освоения дисциплины (модуля). 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;
- типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений и уровня овладения формируемыми компетенциями в процессе освоения дисциплины (модуля).

ФОС является приложением к данной программе дисциплины (модуля).

7. Методические указания для обучающихся по освоению дисциплины

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

Дисциплина (модуль) построена по тематическому принципу, каждая тема представляет собой логически заверченный раздел.

Практические занятия проводятся с целью закрепления усвоенной информации, приобретения навыков ее применения при решении практических задач 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. Котова Л.В. Сборник задач по дисциплине «Методы и средства защиты информации» Электронный ресурс: учебное пособие / Л.В. Котова. – М.: Московский педагогический государственный университет, 2015. – 44 с. – Книга находится в базовой версии ЭБС IPRbooks. – ISBN 978-5-4263-0221-1

2. Ищукова, Е. А. Криптографические протоколы и стандарты: учебное пособие / Е.А. Ищукова, Е.А. Лобова; Министерство образования и науки РФ; Южный федеральный университет; Инженерно-технологическая академия. – Таганрог: Издательство Южного федерального университета, 2016. – 80 с.: ил. – <http://biblioclub.ru/>. – Библиогр. в кн. – ISBN 978-5-9275-2066-4

8.1.2. Перечень дополнительной литературы:

1. Санников, Лапони́на, О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия: учебное пособие / О.Р. Лапони́на. – Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия, 2020-07-28. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 242 с. – Книга находится в базовой версии ЭБС IPRbooks. – ISBN 5-9556-00020-5

2. Молдовян А.А. Протоколы аутентификации с нулевым разглашением секрета [Электронный ресурс] / Молдовян А.А., Молдовян Д.Н., Левина А.Б. – Электрон. текстовые данные. – Санкт-Петербург: Университет ИТМО, 2016. – 55 с. – Режим доступа: <http://www.iprbookshop.ru/68058.html>.

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

1. Лапони́на О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия Электронный ресурс: учебное пособие / О.Р. Лапони́на. – Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия, 2020-07-28. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 242 с. – Книга находится в базовой версии ЭБС IPRbooks. – ISBN 5-9556-00020-5

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

1. База знаний и набор вычислительных алгоритмов WolframAlpha <https://www.wolframalpha.com/>

2. Лекториум – Онлайн-курсы и медиатека видеолекций на русском языке <https://lektorium.tv/>

3. Электронно-библиотечная система IPRbooks <https://iprbooks.ru/>

4. Википедия – Свободная энциклопедия <https://ru.wikipedia.org/>

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

На семинарских и практических занятиях студенты представляют презентации, подготовленные ими в часы самостоятельной работы.

Информационные справочные системы:

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

1. База знаний и набор вычислительных алгоритмов WorframAlpha <https://www.wolframalpha.com>

2. Лекториум – Онлайн-курсы и медиатека видеолекций на русском языке <https://lektorium.tv/>

3. Электронно-библиотечная система IPRbooks <https://iprbooks.ru/>

4. Википедия – Свободная энциклопедия <https://ru.wikipedia.org/>

Программное обеспечение:

1. Операционная система: Microsoft Windows 8: 2013-02(3000). Бессрочная лицензия. Договор № 01-эа/13 от 25.02.2013. Окончание бесплатной поддержки – 2023-01 ИЛИ Операционная система: Microsoft Windows 10: 2016-08(20), 2017-10(67), 2018-01(18), 2018-04(6), 2018-05(6), 2019-02(7). Бессрочная лицензия. Договоры № 27-эа/16 от 02.08.2016. и № 0321100021117000009_229123 от 10.10.2017. На текущий момент

2. Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). MicrosoftOfficeStandard 2013: договор № 01-эа/13 от 25.02.2013г., Лицензирование Microsoft Office <https://support.microsoft.com/ru-ru/lifecycle/search/16674> Дата начала жизненного цикла 09.01.2013г.; набор обновлений Office 2013 Service Pack 1 Дата начала жизненного цикла 25.02.2014г., Дата окончания основной фазы поддержки 10.04

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

Лекционные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: переносной ноутбук, проектор, доска магнитно-маркерная Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин
Практические занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: переносной ноутбук, проектор, доска магнитно-маркерная
Самостоятельная работа	Компьютеры с выходом в Интернет и обеспечением доступа в электронную информационно-образовательную среду организации

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 (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины (модуля) 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 (модуля) обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающего студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать 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, оказывающего студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать 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 (Bigbluebutton, Microsoft Teams, 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.