

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Александровна

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

Дата подписания: 19.06.2026 15:16:51

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, кандидат физико-
математических наук, доцент
Грובה Т.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Математическое и программное обеспечение защиты информации

Направление подготовки 01.04.02 Прикладная математика и информатика

Направленность (профиль) Математическое моделирование

Форма обучения очная

Год начала обучения 2026

Реализуется в 2 семестре

Разработано

Кандидат физико-математических
наук, доцент кафедры
математического моделирования
Ионисян А.С.

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины (модуля)

Цель изучения дисциплины: математическое и программное обеспечение защиты информации

Задачи освоения дисциплины:

1. Современные проблемы информационной безопасности.
2. Общесистемные аспекты криптологии. Основные понятия криптологии.
3. Модулярная арифметика.
4. Криптографические алгоритмы, симметричные шифры,
5. асимметричное шифрование, электронная цифровая подпись
5. криптографический алгоритм Рабина,
6. забывчивый протокол передачи данных,
7. доказательство с нулевым разглашением,
8. протокол Фиата-Шамира.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина изучается в вариативной части цикла дисциплин.

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

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-7. Способен управлять информацией с использованием цифровых средств и алгоритмов обработки данных для решения задач профессиональной деятельности	ИД-1 ПК7 Проводит рецензирование научных статей, авторефератов и диссертаций, составление научных обзоров, рефератов и библиографии с использованием цифровых средств. ИД-2 ПК7 Решает задачи профессиональной деятельности с использованием цифровых средств и алгоритмов обработки данных	Студент изучит современные проблемы информационной безопасности, общесистемные аспекты криптологии, основные понятия криптологии, модулярная арифметику, криптографические алгоритмы, симметричные шифры, асимметричное шифрование, электронная цифровая подпись, криптографический алгоритм Рабина, забывчивый протокол передачи данных, доказательство с нулевым разглашением, протокол Фиата-Шамира.
	ИД-3 ПК7 Занимается подготовкой научных и научно-технических публикаций по тематике проводимых исследований	Студент сможет на практике управлять информацией с использованием цифровых средств и алгоритмов обработки данных для решения задач профессиональной деятельности

4. Объем учебной дисциплины (модуля) и формы контроля

Объем занятий:	З.е.	Акад. ч.	Из них в форме практической подготовки
Всего:	2	72	

Из них аудиторных:		32	
Лекций		16	
Лабораторных работ			
Практических занятий		16	
Самостоятельной работы		40	
Формы контроля:			
Зачет с оценкой			
Реферат			
Курсовая работа			
Экзамен			

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

5.1 Тематический план дисциплины (модуля)

№	Раздел (тема) дисциплины	Реализуемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
4 семестр							
1.	Современные проблемы информационной безопасности.	ИД-1 ПК7 ИД-2 ПК7 ИД-3 ПК7	2	2			
2.	Модулярная арифметика.	ИД-1 ПК7 ИД-2 ПК7 ИД-3 ПК7	2	4			
3.	Криптографические алгоритмы. симметричные шифры асимметричное шифрование криптографический алгоритм Рабина забычивый протокол передачи данных доказательство с нулевым разглашением протокол Фиата-Шамира.	ИД-1 ПК7 ИД-2 ПК7 ИД-3 ПК7	12	10			
	ИТОГО за семестр		16	16			40
	ИТОГО		16	16			40

5.5 Технологическая карта самостоятельной работы обучающегося

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
2 семестр					
ПК-7	Самостоятельное изучение литературы	Отчет по проделанной работе	Собеседование		30
Итого за семестр			40		40
Итого			40		40

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

Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине 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.

Лекционный материал посвящен рассмотрению ключевых, базовых положений курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов *(включается при наличии соответствующих занятий)*.

Практические занятия проводятся с целью закрепления усвоенной информации, приобретения навыков ее применения при решении практических задач в соответствующей предметной области *(включается при наличии соответствующих занятий)*.

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.

Промежуточная аттестация проводится в форме зачета

8. Учебно-методическое и информационное обеспечение дисциплины

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

8.1.1. Перечень основной литературы:

1. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях : монография / Н.И. Червяков, А.А. Коляда, П.А. Ляхов, М.Г. Бабенко, И.Н. Лавриненко, А.В. Лавриненко. - Москва : Физматлит, 2017. - 400 с. : табл., граф., схем. - <http://biblioclub.ru/>. - Библиогр. в кн. - ISBN 978-5-9221-1716-6
2. Обработка информации в системе остаточных классов (СОК) : учебное пособие / Министерство образования и науки РФ ; Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет» ; авт.-сост. Н. И. Червяков ; авт.-сост. П. А. Ляхов ; авт.-сост. Л. Б. Копыткова ; авт.-сост. А. В. Гладков. - Ставрополь : СКФУ, 2016. - 225 с.

1.1.2. Перечень дополнительной литературы:

1. Введение в криптографию / [В. В. Ященко и др.] ; под ред. В. В. Ященко. - 3-е изд., испр. - М. : МЦНМО-ЧеРо, 2000. - 288 с. - (Новые математические дисциплины). - Прил.: с. 251-287. - ISBN 5-900919-65-0
2. Кочеров, Ю. Н. Разработка методов и алгоритмов разделения и восстановления данных в модулярных пороговых структурах для распределенных вычислительных сетей : монография / Ю.Н. Кочеров, Н.И. Червяков ; Министерство образования и науки РФ. - Ставрополь : СКФУ, 2016. - 239 с. : ил. - <http://biblioclub.ru/>. - Библиогр. с. 105-115

1.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Обработка информации в системе остаточных классов (СОК) : учебное пособие / Министерство образования и науки РФ ; Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет» ; авт.-сост. Н. И. Червяков ; авт.-сост. П. А. Ляхов ; авт.-сост. Л. Б. Копыткова ; авт.-сост. А. В. Гладков. - Ставрополь : СКФУ, 2016. - 225 с.

1.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. электронная энциклопедия википедия [электронный ресурс] // www.wikipedia.ru

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

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. 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	электронная энциклопедия википедия [электронный ресурс] // www.wikipedia.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 (модулю)

Учебные аудитории для проведения учебных занятий, оснащены оборудованием и техническими средствами обучения. Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде. Специализированная мебель и технические средства обучения, служащие для представления учебной информации.

Материально-техническая база обеспечивает проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, научно-исследовательской работы обучающихся (переносной ноутбук, переносной проектор, компьютеры с необходимым программным обеспечением и выходом в интернет).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

11. Особенности освоения дисциплины (модуля) 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, оказывающий 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, оказывающий 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.

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, MicrosoftTeams, 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.