

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
Теоретико-числовые методы в криптографии

Специальность	10.05.01 Компьютерная безопасность
Специализация	Информационно-аналитическая и техническая экспертиза компьютерных систем
Форма обучения	очная
Год начала обучения	2026
Реализуется в семестре	4

Разработано:

Петросян Светлана Мартиковна,
старший преподаватель кафедры
вычислительной математики и
кибернетики

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины

Целью изучения дисциплины "Теоретико-числовые методы в криптографии" является формирование общепрофессиональной компетенции студента по специальности 10.05.01 Компьютерная безопасность путём получения базовых знаний и навыков в построении сетей и систем передачи информации.

Задачи освоения дисциплины «Теоретико-числовые методы в криптографии» является:

- обучение студентов основным алгебраическим, аналитическим и вероятностным методам анализа криптосистем;
- формирование у студентов навыков разработки эффективных алгоритмов для решения прикладных задач;
- мотивация деятельности исследовательского характера для развития творческих способностей студентов.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к обязательным дисциплинам обязательной части программы специалитета. Ее освоение происходит в 4 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-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовать процедуры решения задач профессиональной деятельности	ИД-1 ОПК-3 использует математические методы для решения типовых прикладных задач	Применять теоретико-числовые методы для решения прикладных задач, производить основные логические операции в исчислении высказываний.
	ИД-2 ОПК-3 разрабатывает, обосновывает и реализовывает процедуры решения задач профессиональной деятельности на основании математических методов и моделей	Реализовывать свойства представлений булевых и многозначных функций формулами в различных базисах; решать типовые математические задачи, использовать теоретико-числовые методы при решении профессиональных задач.

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	32
Лабораторных работ/из них практическая подготовка	32
Практических занятий/из них практическая подготовка	32
Самостоятельная работа	12
Формы контроля	
Экзамен	36

* 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		
4 семестр							
1	Нахождение наибольшего общего делителя Алгоритм Евклида классического деления. Расширенный алгоритм Евклида. Нахождение обратных элементов в кольце целых чисел. Применение метода Евклида для шифрования RSA.	ОПК-3 ИД-1 ОПК-3					собеседование
2	Арифметические операции над целыми числами Арифметика по модулю (сложение, вычитание, умножение). Возведение в степень по модулю. Китайская теорема об остатках. Быстрое возведение в степень бинарным методом.	ОПК-3 ИД-1 ОПК-3					собеседование
3	Решение сравнений второй степени Основные типы квадратных сравнений. Приведение к каноническому виду. Метод решета для нахождения корней квадратичных сравнений. Решето Ферма и его модификации.	ОПК-3 ИД-1 ОПК-3					собеседование

4	Умножение методом Карацубы-Офмана Идея рекурсивного разбиения. Формула Карацубы для трех членов. Сравнительный анализ сложности классических методов и метода Карацубы. Реализация на примере умножения длинных чисел.	ОПК-3 ИД-1 ОПК-3					собеседование
5	Алгоритм быстрого преобразования Фурье Представление сигнала в частотной области. Быстрая свёртка и обратное преобразование Фурье. Применение БПФ в криптографии и обработке сигналов. Комплексные числа и их использование в быстрых алгоритмах.	ОПК-3 ИД-1 ОПК-3					собеседование
6	Алгоритм Шенхаге-Штрассена для умножения целых чисел Особенности реализации сверхбыстрого умножения с использованием БПФ. Время работы алгоритма. Ограничения применимости метода для коротких чисел. Совмещение с другими методами оптимизации.	ОПК-3 ИД-1 ОПК-3					собеседование
7	Вероятностные алгоритмы проверки чисел на простоту Тест Миллера-Рабина. Тест Соловея-Штрассена. Вероятностные особенности каждого теста и погрешность результатов. Как увеличить надёжность тестов многократным выполнением.	ОПК-3 ИД-1 ОПК-3					собеседование

8	Детерминированные алгоритмы проверки чисел на простоту Метод пробных делений. Алгоритм Агравалья-Каяла-Саксены (AKS-тест). Детерминированные ограничения и практичность AKS-теста. Сложность детерминированных проверок и преимущества перед вероятностными.	ОПК-3 ИД-1 ОПК-3					собеседование
9	Разложение чисел на множители Метод факторизации Ферма. $p-1$ -метод Полларда. Квантовый алгоритм Шора и перспективы квантового разложения чисел. Современное состояние исследований в области эффективных методов факторизации.	ОПК-3 ИД-1 ОПК-3					собеседование
ИТОГО за 4 семестр			32	32	32	12	

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. Тебуева, Ф.Б. Теоретико-числовые методы в криптографии Электронный ресурс: учебное пособие / сост. Ф.Б. Тебуева; В.О. Антонов. – Ставрополь: Северо-Кавказский федеральный университет, 2017. – 107 с. – Книга находится в базовой версии ЭБС IPRbooks.

2. Теоретико-числовые методы в криптографии Электронный ресурс : учебное пособие. специальность 10.05.01 компьютерная безопасность. - Ставрополь : СКФУ, 2017. - 107 с.

8.1.2. Перечень дополнительной литературы:

1. Введение в теоретико-числовые методы криптографии: учеб. пособие / [М.М. Глухов, И.А. Круглов, А.Б. Пичкур и др.]. – СПб.: Лань, 2011. - 400 с.: ил. – (Учебники для вузов. Специальная литература). – На учебнике гриф: Доп.УМО. – Библиогр.: с. 382-389. – ISBN 978-5-8114-1116-0

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

1. Методические указания по выполнению самостоятельных работ по дисциплине "Теоретико-числовые методы в криптографии": для студентов направления 10.05.01 «Компьютерная безопасность»: специализация «Информационно-аналитическая и техническая экспертиза компьютерных систем». – Ставрополь: СКФУ, 2023.

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

1. <http://biblioclub.ru>
2. <http://www.iprbookshop.ru>

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. <http://biblioclub.ru>
2. <http://www.iprbookshop.ru>

Программное обеспечение:

1	Операционная система: Microsoft Windows 8: Бессрочная лицензия. Договор № 01-эа/13 от 25.02.2013.
2	Операционная система: Microsoft Windows 10: Бессрочная лицензия. Договор № 544-21 от 08.06.2021.
3	Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). Microsoft Office Standard 2013: договор № 01-эа/13 от 25.02.2013г., Лицензия Microsoft Office https://support.microsoft.com/ru-ru/lifecycle/search/16674

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
Лабораторные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: HP d330m/P2.4/40ac/256E/4 EURO Блок питания Видео.МОН.ТС-4412А Вольтметр ВЗ-38В Генератор GAG -810 Генератор г4-151 ЖК-монитор 17"Samsung 740 N Монитор 17 TFT" Филипс Монитор 17"ТЕТ Осциллограф с 1-93 Сист.блок HP D31m/P18A/40k/256AC RUSS/XP Сист.блок P4-2.66GHz256MB40GB CDRW-DVD Сист.блок на Intel Pentium 775 Core 2 Duo E4300/1024Mb/80Gb SATA/SVGA/DVD+RW
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, 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, 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 (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.