Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 30.06.2025 14:04:54
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «ТВЕРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Утверждаю:
Руководитель ООП
_____Малышкина О.В.
«30» мая 2025 г.

Рабочая программа дисциплины (с аннотацией)

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Для студентов 3 курса очной формы обучения

Уровень образования
СПЕЦИАЛИТЕТ

Составитель: к.ф.-м.н., доцент Ю.А. Малышкин

Тверь, 2025

I. Аннотация

1. Цель и задачи дисциплины

Цель освоения дисциплины - формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области проектирования и построения криптографических систем, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины являются:

1) получение базовых знаний и умений, связанных с основными понятиями в сфере теоретико-числовых методов в криптографии;

2) изучение общих принципов анализа и назначения различных алгоритмов;

3) освоение методологии решений прикладных задачах с помощью теоретико-числовых методов.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Алгебра», «Математическая логика и теория алгоритмов», «Языки программирования».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 4 зачетные единицы, 144 академических часов, в том числе:

контактная аудиторная работа: лекции – 34 часов, в т.ч. практическая подготовка – 0 часов;

лабораторные занятия – 34 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 76 часа, в том числе контроль 27 часов.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	**ОПК-8.1** Применяет основы теории чисел в криптографии и других дисциплинах
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах,	**ОПК-9.1** Использует криптографические алгоритмы на практике при решении задач криптографическими методами

компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации	
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	**ОПК-10.1.** Сравнивает разные криптографические алгоритмы умеет выбирать оптимальный для данной задачи алг

5. Форма промежуточной аттестации и семестр прохождения – экзамен в 6 семестре.

6. Язык преподавания русский**.**

II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Очная форма обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)			Самостоятельная работа, в том числе Контроль (час.)
		Лекции	Практические занятия		
			всего	в т.ч. практическая подготовка	
Раздел 1. Элементы теории чисел	38	10	8	0	20
Раздел 2. Применение теории чисел в криптографии	106	24	22	4	56
ИТОГО	144	34	30	4	76

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии

Раздел 1. Элементы теории чисел	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция.
Раздел 2. Применение теории чисел в криптографии	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения <u>текущей аттестации</u>

ОПК-8.1; ОПК-9.1; ОПК-10.1

<u>Задания для практических (семинарских) занятий</u>

Раздел I.

Задание 1 (ОПК-8.1; ОПК-9.1; ОПК-10.1): Решить уравнение в целых числах:

$1201u + 2383v = 1$.

Задание 2 (ОПК-8.1; ОПК-9.1; ОПК-10.1):

Вычислить $3^{175} \pmod{263}$.

Раздел II.

Задание 1 (ОПК-8.1; ОПК-9.1; ОПК-10.1):

Вычислить символ Лежандра $\left(\frac{219}{383}\right)$.

Задание 2 (ОПК-8.1; ОПК-9.1; ОПК-10.1):

Использовать p-1 метод факторизации Полларда для разложения на простые множители числа $n = 74951$.

Оценочные материалы для проведения <u>промежуточной аттестации</u>

Проверяемые индикаторы достижения компетенций: **ОПК-8.1; ОПК-9.1; ОПК-10.1**

Каждый студент решает индивидуальное задание и отвечает на теоретический вопрос.

Примерные вопросы к экзамену

1. Алгоритм Евклида и решение линейных уравнений с двумя переменными в целых числах
2. Быстрое возведение в степень по простому модулю
3. Задача дискретного логарифма.
4. Обмен ключами Диффи-Хеллмана.
5. Публичная криптосистема Эль-Гамаля
6. Китайская теорема об остатках

7. Квадратные корни по модулю произведения двух простых чисел
8. Публичная криптосистема RSA
9. Проверка числа на простоту
10. p-1 алгоритм факторизации Полларда
11. Факторизация с помощью разности квадратов
12. Символы Лежандра и Якоби
13. Цифровая подпись RSA
14. Цифровые подписи Эль-Гамаля и DSA
15. Эллиптические кривые над полем вещественных чисел.
16. Эллиптические кривые над конечными полями
17. Задача дискретного логарифма для эллиптических кривых
18. Обмен ключами Диффи-Хеллмана для эллиптических кривых
19. Публичная криптосистема Эль-Гамаля для эллиптических кривых
20. Использование эллиптических кривых для создания цифровых подписей
21. Целочисленные решетки и связанные с ними задачи
22. Публичная криптосистема GGH
23. Цифровая подпись GGH
24. Кольца многочленов
25. Публичная криптосистема NTRU

Вид и способ проведения промежуточной аттестации: индивидуальный устный опрос сочетается с самостоятельной практической работой студента.

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – **5** баллов. Для получения положительной оценки на экзамене необходимо выполнить задачу и ответить на теоретический вопрос с суммарной оценкой не менее 3-х балов.

5 баллов:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется полное верное решение задачи, включающее правильный ответ.

4 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Дано верное решение задачи, но в решении имеются неверные записи И/ИЛИ арифметические ошибки.

3 балла:

Ответ демонстрирует знание и корректное использование терминологии. Решение содержит фактические ошибки, не искажающие общего смысла.

0-2 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Решение не дано ИЛИ дано неверное решение.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429092

Криптографические методы защиты информации : лабораторный практикум / Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет», Министерство образования и науки Российской Федерации ; авт.-сост. И.А. Калмыков, Д.О. Науменко и др. - Ставрополь : СКФУ, 2015. - 109 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458059

б) Дополнительная литература:

Василенко О. Н. Теоретико-числовые алгоритмы в криптографии (2-е издание, дополненное) : монография / О. Н. Василенко. - 2-е изд., доп. - Москва : МЦНМО, 2006. - 336 с. - Режим доступа:
: https://biblioclub.ru/index.php?page=book&id=61814

Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. - Компьютерная безопасность. Криптографические методы защиты. - Электрон. дан. (1 файл). - Саратов : Профобразование, 2019. - 446 с. – Режим доступа: http://www.iprbookshop.ru/87998.html

2) Программное обеспечение

Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus	бесплатно
OpenOffice	бесплатно
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

3) Современные профессиональные базы данных и информационные справочные системы

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.

2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.

3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.

4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.

5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».

www.fstec.ru Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

http://www.intuit.ru/ Национальный Открытый Университете «ИНТУИТ»

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации по организации самостоятельной работы студентов

На лекциях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам.

Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить, что часы для самостоятельной работы, из всего объема времени затраченного на дисциплину, будут превосходить иные виды работ. Важно продумать стиль фиксации нового и важного материала.

Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте и в личном кабинете электронной образовательной среды (LMS).

Требования к рейтинг-контролю для студентов очной формы обучения.

Текущая работа студентов очной формы обучения оценивается в 60 баллов, которые распределяются между двумя модулями (периодами обучения) следующим образом:

Модуль (период обучения)	Максимальная сумма баллов в модуле	Максимальная сумма баллов за работу на практических занятиях	Максимальный балл за рейтинговую контрольную работу
1	30	10	20
2	30	10	20

Правила формирования рейтинговой оценки и шкалу пересчета рейтинговых баллов в оценку на экзамене см. в «Положении о рейтинговой системе обучения в ТвГУ»:

https://tversu.ru/sveden/files/204-R_Pologhenie_o_reytingovoy_sisteme_obucheniya_v_TvGU.pdf

VII. Материально-техническое обеспечение

Учебный процесс по данной дисциплине проводится в аудиториях, оснащенных мультимедийными средствами обучения. Для организации самостоятельной работы студентов необходимо наличие персональных компьютеров с доступом в Интернет.

Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Помещение для самостоятельной работы, учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, практики Компьютерный класс 203а 170002, г.Тверь, Садовый пер-к, д. 35.	Набор учебной мебели, меловая доска, Переносной ноутбук, Интерактивная система Smart Board 660iv со встроенным проектором	Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus –бесплатно; OpenOffice – бесплатно; Многофункциональный редактор ONLYOFFICE бесплатное ПО- бесплатно; ОС Linux Ubuntu бесплатное ПО-бесплатно
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, *у*чебная аудитория 224, 170002, г.Тверь, Садовый пер-к, д. 35	Набор учебной мебели, меловая доска, Переносной ноутбук, Мультимедийный проектор BenQ MP 724 с потолочным креплением и экраном 1105	Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus –бесплатно; OpenOffice – бесплатно; Многофункциональный редактор ONLYOFFICE бесплатное ПО- бесплатно; ОС Linux Ubuntu бесплатное ПО-бесплатно

Наличие учебно-наглядных пособий, презентаций для проведения занятий лекционного и семинарского типа, обеспечивающих тематические иллюстрации.

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	Обновленный	Описание внесенных	Дата и протокол

	раздел рабочей программы дисциплины (или модуля)	изменений	заседания кафедры, утвердившего изменения
1.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы.	Протокол № 11 от 26.06.2013
2.	VII. Методические указания для обучающихся по освоению дисциплины	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 10 от 24.06.2014
3.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы. Обновление ссылок из ЭБС.	Протокол № 1 от 27.09.2015
4.	VII. Методические указания для обучающихся по освоению дисциплины.	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 1 от 01.09.2016
5.	I - X	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 6 от 28.02.2017
6.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Дополнение списков. Обновление ссылок из ЭБС.	Протокол № 1 от 01.09.2018
7.	I - VIII	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 10 от 29.06.2021
8.	V. Учебно-методическое и информационное обеспечение	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023

	дисциплины		
9.	II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий, IV. Оценочные материалы для проведения текущей и промежуточной аттестации	Корректировка наименований разделов и тем. Корректировка оценочных материалов	Протокол № 7 от 7.03.2024
10.	II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий,	Корректировка содержания дисциплины	Протокол № 8 от 20.05.2025