Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП:

_____ Н.А. Семыкина

«_9_» _06_ 2023 г.

Рабочая программа дисциплины (с аннотацией)

Теоретико-числовые методы в криптографии

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов 4 курса очной формы обучения

Уровень высшего образования

СПЕЦИАЛИТЕТ

Составители:

ст. преподаватель С.А. Желтов.

Тверь 2023

I. Аннотация

1. Наименование дисциплины (модуля) в соответствии с учебным планом
Теоретико-числовые методы в криптографии.

2. Цель и задачи дисциплины (модуля)
Целью освоения дисциплины (модуля) является:
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 (модуля) являются:

- получение базовых знаний и умений, связанных с основными теоретико-числовыми методами в криптографии;
- получение теоретических знаний о роли и назначении различных алгоритмов;
- получение теоретических знаний и практических навыков о основных прикладных задачах, решаемых с помощью теоретико-числовых методов;

3. Место дисциплины (модуля) в структуре ООП

Дисциплина входит в базовую часть профессионального цикла. Для освоения дисциплины студент должен владеть основными понятиями криптографии, информационной безопасности. Необходимы знания, умения и компетенции, полученные студентами на занятиях по дисциплинам, языки программирования, криптографические методы защиты информации, алгебра, математическая логика и теория алгоритмов. Знания и практические навыки, полученные из курса, используются студентами при прохождении производственной и преддипломной практики, а также при разработке курсовых и дипломных работ.

4. Объем дисциплины (или модуля):
___2___ зачетных единиц, __72__ академических часов, **в том числе контактная работа:** лекции _18__ часов, практические занятия _18____ часов, , **самостоятельная работа:** ___36__ часов.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	**Планируемые результаты обучения по дисциплине (модулю)**

ОПК-3 – способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и в иных источниках информации	**Владеть:** криптографической терминологией. **Уметь:** уметь учитывать современные достижения информационных технологий в своей профессиональной деятельности. **Знать:** о видах информации, подлежащей шифрованию.
Базовый **ПСК-2.1.** способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	**Владеть:** навыками применения теории чисел в криптографии; навыками применения основных вычислительных алгоритмов в кольцах вычетов и кольцах многочленов. **Уметь:** применять теоретико-числовые методы и алгоритмы для защиты информации; исследовать и решать системы сравнений по произвольному модулю; представлять действительные числа цепными дробями; строить большие простые числа, применять алгоритмы проверки чисел на простоту; построения больших простых чисел; применять алгоритмы разложения чисел и многочленов на множители. **Знать:** теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации.

6. Форма промежуточной аттестации: зачет.

7. Язык преподавания русский**.**

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

Для студентов очной формы обучения

Учебная программа – наименование разделов и тем	**Всего (час.)**	**Контактная работа (час.)**		**Самостоятельная работа (час.)**
		Лекции	Практические (лабораторные) занятия	
Раздел 1. Сложность алгоритмов				
Тема 1.1. Оценка сложности арифметических операций. Функции оценки сложности. Классификация вычислительных алгоритмов	14	4	4	6
Тема 1.2. Сложность вычислений в кольце вычетов	6	2	2	2
Тема 1.3. Вычисления с многочленами.	6	2	2	2
Раздел 2. Элементы теории чисел.				
Тема 2.1. Непрерывные (цепные) дроби и их свойства	12	4	4	4
Тема 2.2. Квадратичные вычеты и невычеты. Символ Лежандра	14	4	4	6
Тема 2.3. Символ Якоби	6	2	2	2
Тема 2.4. Распределении простых чисел	9	2	2	2
Тема 2.5. Алгоритмы генерации простых чисел	18	6	6	6
Тема 2.6. Алгоритмы проверки простоты числа	14	4	4	6
ИТОГО	**106**	**30**	**30**	**36**

Учебная программа

Раздел 1. СЛОЖНОСТЬ АЛГОРИТМОВ

Тема 1.1. Оценка сложности арифметических операций. Функции оценки сложности. Классификация вычислительных алгоритмов.

Понятие сложности алгоритма. Двоичные операции. Сложность арифметических операций с целыми числами. Оценки функций сложности. Классификация вычислительных алгоритмов. Оценка сложности программ.

Тема 1.2. Сложность вычислений в кольце вычетов

Сложность арифметических операций в кольце вычетов. Использование модульной арифметики.

Тема 1.3. Вычисления с многочленами

Вычисление значений многочлена. Алгоритм Руффини-Горнера.

Раздел 2. Элементы теории чисел.

Тема 2.1. Непрерывные (цепные) дроби и их свойства.

Непрерывные (цепные) дроби и их свойства. Свойства непрерывных дробей. Свойства подходящих дробей. Представление действительных чисел непрерывными дробями. Связь числа $\alpha \in R$ и подходящей дроби $[a_1,...,a_n] = \frac{P_n}{Q_n}$, $n = 1,2,...$.

Тема 2.2. Квадратичные вычеты и невычеты. Символ Лежандра

Квадратичные вычеты и невычеты. Свойства квадратичных вычетов. Символ Лежандра и его свойства. Квадратичный закон взаимности Гаусса. Алгоритм вычисления значения символа Лежандра.

Тема 2.3. Символ Якоби

Символ Якоби. Свойства символа Якоби. Алгоритм вычисления символа Лежандра с помощью символа Якоби.

Тема 2.4. Распределении простых чисел

Теорема Чебышева о распределении простых чисел.

Тема 2.5. Алгоритмы генерации простых чисел

n+1 методы построения больших чисел

Тема 2.6. Алгоритмы проверки простоты числа

n-1 методы проверки простоты. n+1 методы проверки простоты

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (или модулю)

Самостоятельная работа обучающихся направлена на освоение учебного материала и развитие практических умений. Самостоятельная работа включает следующие виды самостоятельной работы студентов: работа с рекомендованной литературой и документацией; выполнение практических заданий; подготовка к контрольным .

Тематика рефератов и методические рекомендации по их написанию.

1. тест ферма
2. Тест Соловея-Штрассена
3. тест Миллера-Рабина
4. Метод Ваулина
5. Метод Шермана Лемана
6. Метод Полларда-Штрассена
7. ro-метод Полларда
8. метод квадратичного решета
9. p-1 метод Полларда

Вопросы для контрольных тестов и самоконтроля.

1. Что такое сложность алгоритма, ее виды?

2. Приведите классификацию алгоритмов по вычислительной сложности

3. Назовите алгоритмы генерации простого числа.

4.. Назовите алгоритмы проверки простоты числа

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (или модулю)

1.Типовые контрольные задания для проверки уровня сформированности компетенции ОПК – 3.

Рассматривается трехкомпонентной структура компетенции: знать, уметь, владеть.

При этом под указанными категориями понимается:

- «знать» – воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты;
- «уметь» – решать типичные задачи на основе воспроизведения стандартных алгоритмов решения;
- «владеть» – решать усложненные задачи на основе приобретенных знаний, умений и навыков, в нетипичных ситуациях

Этап формирования компетенции, в котором участвует дисциплина	**Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)**	**Показатели и критерии оценивания компетенции, шкала оценивания**
Базовый		
владеть	Основными теории чисел и теории алгоритмов	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части описания из-за логической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов
	Алгоритмами реализующими вычислительные операции над длинными числами	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за логической ошибки – 1 балл • Решение не дано ИЛИ

		дано неверное решение – 0 баллов
уметь	Описывать схемы и алгоритмы реализующие вычислительные операции над длинными числами	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
	Определить сложность алгоритмов.	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за логической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов
знать	Основные алгоритмы генерации простых чисел.	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
	Основные алгоритмы проверки просты чисел.	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов

2.Типовые контрольные задания для проверки уровня сформированности компетенции ПСК-2.1.

владеть	навыками доказательств утверждений и теорем	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов
уметь	Формулировать (описывать) алгоритмы схемы реализующие методы проверки просты и генерации простых чисел	• Имеется полное верное решение, включающее правильный ответ – 3 балла • Дано верное решение, но в решении имеются неверные записи, не отделенные от решения – 2 балла • Имеется верное решение части программы из-за алгоритмической ошибки – 1 балл • Решение не дано ИЛИ дано неверное решение – 0 баллов
знать	Оценки сложности основных вычислительных алгоритмов используемых в криптографии	• Факты и примеры в полном объеме обосновывают выводы – 2 балла • Допущена фактическая ошибка, не приведшая к существенному искажению смысла – 1 балл • Допущены фактические и логические ошибки, свидетельствующие о непонимании темы – 0 баллов

При оценивании результатов освоения дисциплины применяется «рейтинговая» технология (балльно-накопительная) система. Оценка уровня сформированности компетенций осуществляется в процессе следующих форм контроля:

1) **следящего** (проводится оценка выполнения студентами заданий в ходе аудиторных занятий). Дает возможность квалифицировать степень сформированности знаний, умений, навыков, а также их глубину и прочность. Его задача - регулярное управление учебной деятельности студентов и ее корректировка. Он позволяет получать первичную информацию о ходе и качестве

усвоения учебного материала, а также стимулировать регулярную, напряженную и целенаправленную работу студентов. Данный контроль позволяет вовремя выявить пробелы в знаниях и оказать им помощь в усвоении программного материала. Данными формами контроля являются: ответы с места и у доски, проверка работ выполненных в тетради.

2) **текущего** (оценивается работа студентов вне аудиторных занятий). Текущими формами контроля являются: проверка выполнения практических работ, ответы у доски, рефераты, доклады, проверка самостоятельной работы студентов.

3) **промежуточного** (рейтинговые точки) позволяет определять качество изучения студентами учебного материала по разделам и темам. Контроль проводится два раз в семестр. С помощью периодического контроля обобщаются и усваиваются целые темы и разделы, выявляется взаимосвязями с другими разделами, предметами. Контроль охватывает студентов и всей группы и проводится в виде теста, письменных практических работ.

4) **итогового** (зачёт). Максимальная сумма рейтинговых баллов по дисциплине составляет 100 баллов. Студенту, набравшему 50 баллов и выше по итогам работе в семестре, в экзаменационной ведомости и зачетной книжке выставляется оценка «зачтено». Студент, набравший от 20 до 49 баллов включительно, сдаёт зачет в последнюю неделю семестра по данной дисциплине. Баллы, полученные на зачете проставляются в ведомости. Студенту, набравшему меньше 20 баллов, в экзаменационной ведомости выставляется оценка «незачтено». Данному студенту разрешается пересдача зачета по направлению деканата на последней неделе семестра.

Формы контроля

Занятия для студентов очной формы обучения проводятся в 2-м семестре 4 курса и заканчиваются зачетом. Период времени, отведенный на обучение по данной дисциплине, планируется разделить на 2 модуля, каждый из которых заканчивается контрольной точкой. Количество баллов за текущую работу выставляется в соответствии со сложностью темы и количеством заданий, выносимых для практических работ в аудитории и самостоятельных занятий.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы.

Для оценки уровня теоретических и практических знаний используется тест или контрольная работа письменный опрос. Перечень некоторых вопросов теста и практических заданий представлен ниже.

Приводится два варианта из имеющихся двадцати различных вариантов по каждой из рассматриваемых тем.

Вариант 1

1. . Вычислить неприрывную дробь $[2,3,1,6]$

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

Вариант 2

1. Вычислить неприрывную дробь $[1,10,3,8]$
2. Вычислить симол Лежандра $\left(\frac{126}{53}\right)$

ВОПРОСЫ К ЗАЧЕТУ

1. Сложность алгоритмов, методика оценки асимптотической сложности программ.
2. Оценка сложности арифметических операций. Функции оценки сложности и их свойства.
3. Сложность арифметических операций с целыми числами.
4. Сложность операций в кольце вычетов.
5. Модульная арифметика. Китайская теорема об остатках.
6. Вычисления с многочленами.
7. Непрерывные дроби и их свойства.
8. Символ Лежандра и его св-ва.
9. Символ Якоби и его св-ва.
10. Алгоритм вычисления символ Лежандра
11. Алгоритм вычисления символ Якоби
12. Квадратичные вычеты и невычеты. Квадратичный закон взаимности Гаусса.
13. Асимптотический закон распределения простых чисел. Теорема Чебышева о распределении простых чисел.
14. Метод Шермана Лемана
15. ρ-метод Полларда
16. (n+1) м-ды проверки простоты чисел
17. (n-1) м-ды проверки простоты чисел
18. (p-1) м-д факторизации Поллорда
19. Тест ферма

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (или модуля)

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

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

1. 1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.
2. 2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.
3. 3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.
4. 4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.
5. 5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.
6. Информационная безопасность на Report.ru
7. Информационная безопасность / Блог / Хабрахабр
8. Библиотека информационной безопасности
9. Библиотека сетевой безопасности
10. Компьютерная безопасность: уязвимости, ошибки и эксплоиты
11. Построение безопасности в сетях
12. openPGP в России
13. Защита информации

VII. Методические указания для обучающихся по освоению дисциплины (или модуля)

Материал дисциплины распределен по главным разделам (темам). В результате изучения дисциплины у студентов должно сформироваться научное представление о криптографических системах на базе эллиптических кривых. Необходимо выработать системный подход к пониманию процессов преобразования входных данных в приложениях защиты информации. В процессе обучения студенты, наряду с текстами лекций и учебными пособиями, должны пользоваться дополнительными научными изданиями, академическими периодическими изданиями. После каждой лекционной темы рекомендуется проработать вопросы для повторения и самоконтроля. В аспекте

самостоятельной работы рекомендуется составлять конспект. Рекомендуется использовать справочники и руководства.

Для успешного освоения дисциплины важно соблюсти следующие рекомендации: На первой лекции важно обратить внимание на конкретные требования к прохождению и сдаче курса. Активная работа на занятиях, выполнение творческих заданий сформирует о Вас дополнительное положительное представление как об активном участнике познавательного процесса. На данном курсе практические занятия являются самым важным компонентом обучающего процесса. На занятиях 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, настоятельно 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 в библиотеках и системе «Интернет». Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить: без самостоятельной работы невозможно серьезное освоение любого курса. Надо быть готовым к тому, что по времени, затраченном на дисциплину, самостоятельная работа будет превалировать над иными видами работы. 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.

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

Процесс изучения дисциплины включает лекции, практические занятия и самостоятельную работу студента. Во время обучения применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении занятий применяется имитационный подход (метод деловой игры, анализ конкретных ситуаций), когда преподавателем разбирается на конкретном примере проблемная ситуация, все шаги решения задачи студентам демонстрируются при помощи мультимедийной техники. Затем студенты самостоятельно решают аналогичные задания. Так же при проведении занятий применяется частично-поисковый метод: студенты осуществляют поиск решения поставленной проблемы (задачи). При этом постановочные задачи опираются на уже имеющиеся у студентов знания и умения, полученные в предшествующих темах. На занятиях практикуется выполнение заданий в малых группах, письменные работы, работа с раздаточным материалом, привлекаются ресурсы сети Интернет. Курс предусматривает выполнение тестов, контрольных и самостоятельных работ,

письменных домашних заданий. В качестве форм контроля используются различные варианты взаимопроверки и взаимоконтроля.

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

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (или модулю)

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски. Класс ПЭВМ с установленным программным обеспечением.

X. Сведения об обновлении рабочей программы дисциплины (или модуля)

№п.п.	Обновленный раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.	I - X	14.05.2017 Корректировка всех разделов в соответствии с новым стандартом	
2.			
3.			