Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 2023 г.

Рабочая программа дисциплины (с аннотацией)

Методы алгебраической геометрии в криптографии

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 5 курса ОФО

Составитель:
Семыкина Н. А.

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Целью изучения дисциплины является формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области проектирования и построения криптографических протоколов на эллиптических кривых, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

Задачами освоения дисциплины являются:

1) получение базовых знаний и умений, связанных с основными понятиями алгебраической геометрии;

2) получение теоретических знаний о роли и назначении различных криптосистем на базе эллиптических кривых;

3) изучение общих принципов и методов построения криптографических систем на основе эллиптических кривых;

4) изучение различных схем электронной подписи и современных стандартов формирования проверки ЭЦП.

2. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Методы и средства криптографической защиты информации», «Алгебра».

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

3. Объем дисциплины: 3 зачетные единицы, 108 академических часов, в том числе:

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

практические занятия – 17 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 57 часа.

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-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	**ОПК-3.1** Производит стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения	**ОПК-8.1** Применяет основы теории чисел в криптографии и других дисциплинах

безопасности компьютерных систем и сетей	
ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, 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-9.1.** Использует криптографические алгоритмы на практике при решении задач криптографическими методами
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.** Использует методы построения быстрых вычислительных алгоритмов алгебры и теории чисел
ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	**ОПК-2.1.1.** Использует в профессиональной деятельности криптографические алгоритмы и реализует их программно
	ОПК-2.1.2. Разрабатывает рекомендации и предложения по совершенствованию и повышению эффективности защиты информации
ОПК-2.2. Способен разрабатывать и анализировать математические модели механизмов защиты информации	**ОПК-2.2.1.** Выявляет наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы
	ОПК-2.2.2. Разрабатывает математические модели, реализуемые в средствах защиты информации

5. Форма промежуточной аттестации и семестр прохождения – зачет в 9 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	
Тема 1. . Элементы алгебраической геометрии и алгебры.	35	12	4	0	19
Тема 2. Эллиптические кривые в криптографии.	35	12	4	0	19
Тема 3. Формирование и проверка ЭЦП.	38	10	5	4	19
ИТОГО	108	34	13	4	57

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Тема 1. Элементы алгебраической геометрии и алгебры.	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция.
Тема 2. Эллиптические кривые в криптографии:	лекция практическое	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления
Тема 3. Формирование и проверка ЭЦП.	лекция практическое	Дискуссионные технологии, кейс-технология, методы группового решения творческих задач.

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

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

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

Тема I.

Задание 1 (ОПК-3.1, ОПК-10.1): Даны точки $P(13,16)$, $Q(17,3)$, $R(18,20)$ на кривой $E_{23}(1,1)$. Найти точку $\boldsymbol{2P + 3Q - R}$.

Задание 2 (ОПК-3.1, ОПК-10.1): Дана эллиптическая кривая E_{11} (1,6). Найти все точки эллиптической кривой, определить ее порядок и образующий элемент.

Тема II.

Задание 1 (ОПК-8.1, ОПК-9.1): Зашифровать открытый текст { МАГ }. Используется кривая $E_{41}(3,1)$ и генерирующая точка $G = (1, 13)$. Открытый ключ – точка $P_B=(31,23)$. Значения случайных чисел k для букв открытого текста: {3, 2, 3}.

Задание 2 (ОПК-8.1, ОПК-9.1): Дан шифртекст. {(56, 419), (301, 734)}. Используя алфавит для кривой $E_{751}(-1,1)$ и генерирующую точку G= (-1, 1), и зная секретный ключ n_b=10, найти открытый текст.

Тема III.

Задание 1 (ОПК-2.1.1., ОПК-2.1.2., ОПК-2.2.1., ОПК-2.2.2.): Сгенерировать ЭЦП для сообщения с известным значением хэш-свертки h=12, зная секретный ключ подписи $d=12$, при данном значении выбираемого случайным образом числа $k=3$. Используется кривая E_{751} (− 1,1) и генерирующая точка $G = (384, 475)$ порядка q =13.

Задание 2 (ОПК-2.1.1., ОПК-2.1.2., ОПК-2.2.1., ОПК-2.2.2.): Проверить подлинность ЭЦП (r, s) для сообщения с известным значением хэш-свертки h, зная открытый ключ проверки подписи Q.

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

Проверяемые индикаторы достижения компетенций: ОПК-3.1, ОПК-8.1, ОПК-9.1, ОПК-10.1, ОПК-2.1.1., ОПК-2.1.2., ОПК-2.2.1., ОПК-2.2.2.

Каждый студент решает индивидуальное задание и отвечает на теоретический вопрос.

Примерные вопросы к зачету

1. Понятие эллиптической кривой над числовым полем. Группа точек эллиптической кривой
2. Понятие эллиптической кривой над конечным полем. Группа точек эллиптической кривой
3. Эллиптические кривые в криптографии
4. Вычислительные операции в конечных полях
5. Системы шифрования на эллиптических кривых
6. Обмен ключами с использованием эллиптических кривых
7. Протокол Диффи – Хелмана на основе суперсингулярных кривых
8. ЭЦП на эллиптических кривых
9. Атаки на ЭЦП.
10. Алгоритмы генерации эллиптической кривой и выбора точки на ней
11. Задача дискретного логарифмирования на эллиптической кривой
12. Число точек эллиптической
13. Встраивание открытого текста в координату точки
14. Требования к эллиптической кривой
15. Метод Гельфонда
16. Методы встречи посередине
17. Метод Полларда.
18. Алгоритм Ленстре

19. Криптосистема Эль-Гамаля над группой точек эллиптической кривой
20. Криптосистема Месси – Омуры над группой точек эллиптической кривой.

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

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – **3** балла. Для получения зачета необходимо выполнить задачу и ответить на теоретический вопрос с суммарной оценкой не менее 2-х балов.

3 балла:

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.

2 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.

1 балл:

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

0 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

Рацеев, С. М. Математические методы защиты информации / С. М. Рацеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 544 с. — ISBN 978-5-507-47085-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/326153

Алешников С.И. Математические методы защиты информации. Часть 5. Методы алгебраических кривых [Электронный ресурс]: учебное пособие/ С.И. Алешников,

А.А.Смирнов. - М. ; Берлин : Директ-Медиа, 2017. - 358 с. : ил., табл. - Библиогр. в кн. - ISBN 978-5-4475-8780-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457616

б) Дополнительная литература:

Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие для СПО / Б. А. Фороузан ; под редакцией А. Н. Берлина. — Саратов : Профобразование, 2021. — 776 с. — ISBN 978-5-4488-0999-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102192.html

Донгак, Ш. М. Криптография: Практикум : учебное пособие / Ш. М. Донгак. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 64 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163935

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.

6. https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».
7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp;
8. Репозитарий ТвГУ http://eprints.tversu.ru

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

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 100 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	Реферирование, представление научной статьи, создание и отладка кода	Максимальный балл за рейтинговую контрольную работу
1	50	18	12	20
2	50	18	12	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	Столы, стулья, переносной ноутбук, компьютеры	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 Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт

170002, г.Тверь, Садовый пер-к, д. 35. 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* 203, 224, 170002, г.Тверь, Садовый пер-к, д. 35	Столы, стулья, переносной ноутбук, проектор	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 раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол 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 01.09.2017
7.	I - VIII	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 10 от 29.06.2021
8.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023