Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Дальневосточный государственный университет путей сообщения"
(ДВГУПС)

УТВЕРЖДАЮ

Зав.кафедрой
(к902) Высшая математика

Виноградова Полина
Витальевна

27.05.2022

РАБОЧАЯ ПРОГРАММА

дисциплины **Эллиптические системы в криптографии**

для направления подготовки 45.03.04 Интеллектуальные системы в гуманитарной сфере

Составитель(и): к.ф.-м.н., доцент, Авдеева М.О.;к.ф.-м.н., доцент, Коломийцева С.В.

Обсуждена на заседании кафедры: (к902) Высшая математика

Протокол от 11.05.2022г. № 6

Обсуждена на заседании методической комиссии учебно-структурного подразделения: Протокол от 27.05.2022 г. № 8

г. Хабаровск
2022 г.

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры (к902) Высшая математика

Протокол от __ _____ 2023 г. № __
Зав. кафедрой Виноградова Полина Витальевна

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2024 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры (к902) Высшая математика

Протокол от __ _____ 2024 г. № __
Зав. кафедрой Виноградова Полина Витальевна

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры (к902) Высшая математика

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Виноградова Полина Витальевна

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры (к902) Высшая математика

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Виноградова Полина Витальевна

Рабочая программа дисциплины Эллиптические системы в криптографии

разработана в соответствии с ФГОС, утвержденным приказом Министерства образования и науки Российской Федерации от 24.04.2018 № 324

Квалификация **бакалавр**

Форма обучения **очная**

ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144 Виды контроля в семестрах:
в том числе: зачёты с оценкой 6
контактная работа 52
самостоятельная работа 92

Распределение часов дисциплины по семестрам (курсам)

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	32	32	32	32
Контроль самостоятельной работы	4	4	4	4
В том числе инт.	24	24	24	24
Итого ауд.	48	48	48	48
Контактная работа	52	52	52	52
Сам. работа	92	92	92	92
Итого	144	144	144	144

1. АННОТАЦИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Математический аппарат, связанный с эллиптическими кривыми и конечными полями, протоколы криптосистем на эллиптические кривых, рассмотрен механизм выбора эллиптической кривой и точки на ней; кодировка сообщений точками эллиптической кривой.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Код дисциплины:	Б1.О.32
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Математическая логика и теория алгоритмов
2.1.2	Высшая математика
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Распознавание образов

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

ОПК-1: Способен применять в профессиональной деятельности методы математического анализа, логики и моделирования, теоретического и экспериментального исследования в информатике, лингвистике и гуманитарных науках;

Знать:

Основные определения, базовые факты теории информации;

Уметь:

Обосновывать выбор средств для решения конкретных задач; применять полученные решения для математических и лингвистических проблем в рамках теоретических и прикладных задач; структурировать собственные рассуждения, формулировать алгоритмы решения типовых задач;

Владеть:

Основными методами решения типичных теории информации.

ПК-1: Способность разрабатывать новые программы и системы, формулировать задания, использовать средства автоматизации при проектировании информационных систем

Знать:

– возможности современных и перспективных средств разработки программных продуктов, технических средств; методологии разработки программно-го обеспечения и технологии программирования;
– способы выбора, обработки, анализа информации.

Уметь:

– решать типовые задачи путем последовательного воспроизведения алгоритма решения;
– проводить оценку и обоснование рекомендуемых решений;
– применять принципы многоуров-невой организации и проектирования информационных систем на основе концепции открытых систем;

Владеть:

– навыками обработки информации и решения поставленной задачи в стандартных условиях

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел 1. Лекции						
1.1	Основные понятия эллиптических кривых. Математический аппарат связанный с эллиптическими кривыми и конечными полями /Лек/	6	2	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	0	
1.2	Свойства эллиптическх кривых /Лек/	6	2	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
1.3	Арифметические операции на эллиптических кривых /Лек/	6	2	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах

1.4	Механизм выбора эллиптической кривой и точки на ней. Построение криптосистем /Лек/	6	2	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
1.5	Протоколы криптосистем на эллиптические кривых. Проверка чисел на простоту /Лек/	6	2	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
1.6	Функции хэширования и ЭЦП по ГОСТ 34.11-2018 /Лек/	6	2	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
1.7	Решение задачи дискретного логарифмирования на группе точек ЭК /Лек/	6	2	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
1.8	Факторизация чисел с помощью ЭК. Кодировка сообщений точками эллиптической кривой /Лек/	6	2	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	0	
	Раздел 2. Практика						
2.1	Основные алгоритмы теории чисел. Анализ их быстродействия /Пр/	6	4	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	0	
2.2	Мультипликативно обратное для разных модулей. /Пр/	6	4	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	0	
2.3	Сложение и умножение в группе точек ЭК /Пр/	6	4	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
2.4	Алгоритмы вычисления количества точек на ЭК /Пр/	6	4	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
2.5	Алгоритмы криптографической защиты на ЭК. Шифр Эль-Гамаля /Пр/	6	4	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
2.6	Обмен ключами с использованием ЭК. Протокол Диффи-Хеллмана /Пр/	6	4	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
2.7	ЭЦП по ГОСТ 34.11-2018 /Пр/	6	4	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
2.8	Анализ криптографических алгоритмов на ЭК /Пр/	6	4	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	2	Работа в малых группах
2.9	Изучение литературы /Ср/	6	30	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	0	
2.10	Подготовка к практическим занятиям /Ср/	6	18	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	0	
2.11	Подготовка к зачету с оценкой /Ср/	6	36	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	0	

2.12	Подготовка и выполнение РГР /Ср/	6	8	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.2 Э1	0	
	Раздел 3. Зачет						
3.1	/ЗачётСОц/	6	0	ПК-1 ОПК-1	Л1.1 Л1.2Л2.1Л3.1 Э1	0	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Размещены в приложении

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Перечень основной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Романьков В. А.	Алгебраическая криптография: Учебное пособие	Омск: Омский государственный университет, 2013, http://biblioclub.ru/index.php?page=book&id=238045
Л1.2	Рябко Б.Я.	Криптографические методы защиты информации: учеб. пособие	Москва: Горячая линия-Телеком, 2012, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5193

6.1.2. Перечень дополнительной литературы, необходимой для освоения дисциплины (модуля)

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Рябко Б. Я., Фионов А. Н.	Основы современной криптографии и стеганографии	Москва: Горячая линия-Телеком, 2011, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5192

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

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Коломийцева С.В.	Введение в эллиптическую криптографию: метод. пособие по выполнению лабораторной работы	Хабаровск: Изд-во ДВГУПС, 2012,
Л3.2	Виноградова П.В., Деревянко О.С.	Организация и контроль самостоятельной работы студентов: метод. указания по самостоятельной работе студентов по напр. подготовки 45.03.04 "Интеллектуальные системы в гуманитарной сфере"	Хабаровск: Изд-во ДВГУПС, 2021,

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Э1	Электронный каталог НТБ	http://ntb.festu.khv.ru/

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

6.3.1 Перечень программного обеспечения

Matlab Базовая конфигурация (Academic new Product Concurrent License в составе: (Matlab, Simulink,Partial Differential Equation Toolbox) - Математический пакет, контракт 410
Total Commander - Файловый менеджер, лиц. LO9-2108, б/с
Windows 7 Pro - Операционная система, лиц. 60618367
WinRAR - Архиватор, лиц.LO9-2108, б/с
Антивирус Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition - Антивирусная защита, контракт 469 ДВГУПС
Free Conference Call (свободная лицензия)
Zoom (свободная лицензия)

Mathcad Education - University Edition - Математический пакет, контракт 410
Lazarus, свободно распространяемое ПО
6.3.2 Перечень информационных справочных систем
Профессиональная база данных, информационно-справочная система КонсультантПлюс - http://www.consultant.ru

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Аудитория	Назначение	Оснащение
249	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.
343	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи. Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.
3317	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.
1303	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.
423	Помещения для самостоятельной работы обучающихся. зал электронной информации	Тематические плакаты, столы, стулья, стеллажи Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.
3322	Помещения для самостоятельной работы обучающихся. Читальный зал НТБ	Тематические плакаты, столы, стулья, стеллажи Компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС.
109	Компьютерный класс для практических и лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы. Зал инклюзивного образования	комплект учебной мебели: столы, стулья, доска, компьютерная техника с возможностью подключения к сети Интернет, свободному доступу в ЭБС и ЭИОС: Core i5- 650 (3.20GHz), 4 Gb, int Video, 500GB, DVD+RW, ЖК 19", ЖК панель 55", 1 специализированный ПК для инклюзивного образования
1201	Учебная аудитория для проведения занятий лекционного типа	комплект учебной мебели: столы, стулья, доска

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для рационального распределения времени обучающегося по разделам дисциплины и по видам самостоятельной работы студентам предоставляется календарный план дисциплины, а также учебно-методическое и информационное обеспечение, приведенное в данной рабочей программе.
В процессе обучения студенты должны усвоить научные основы предстоящей деятельности, научиться управлять развитием своего мышления. С этой целью они должны освоить различные алгоритмы мышления. Алгоритмы развития мышления выстраиваются так, чтобы знания (закон, закономерность, определение, вывод, правило и т. д.) могли применяться при выполнении заданий (решении задач).
В результате обучения студенты должны иметь опыт как разработки алгоритма применения знаний, так и способности его применения при выполнении заданий по курсу теории.
При обучении используются социально-активные и рефлексивные методы обучения для создания комфортного психологического климата в студенческой группе.

Описание интерактивной формы обучения «Работа в малых группах»
Форма организации учебно-познавательной деятельности, предполагающая функционирование разных малых групп, работающих как над общими, так и над специфическими заданиями преподавателя. Групповая работа стимулирует согласованное взаимодействие между студентами, отношения взаимной ответственности и сотрудничества.
Организация групповой работы:
Учебная группа разбивается на несколько небольших групп - от 3 до 6 человек.
Каждая группа получает свое задание. Задания могут быть одинаковыми для всех групп либо дифференцированными.
Внутри каждой группы между ее участниками распределяются роли.
Процесс выполнения задания в группе осуществляется на основе обмена мнениями, оценками.
Формирование групп.
При комплектовании групп учитываются два признака:
* уровень учебных успехов студентов;
* характер межличностных отношений.
Студентов можно объединить в группы или по однородности (гомогенная группа), или по разнородности (гетерогенная группа) учебных успехов.
В группу должны подбираться студенты, между которыми сложились отношения доброжелательности. Только в этом случае в группе возникает психологическая атмосфера взаимопонимания и взаимопомощи, снимаются тревожность и

страх.
Функции преподавателя:
* Объяснение цели предстоящей работы;
* Разбивка студентов на группы;
* Раздача заданий для групп;
* Контроль за ходом групповой работы;
* Попеременное участие в работе групп, но без навязывания своей точки зрения как единственно возможной, а побуждая к активному поиску.
* После отчета групп о выполненном задании преподаватель делает выводы.
Преимущества групповой работы:
Группа имеет «множество глаз». Каждый участник может увидеть себя и свои проблемы с других точек зрения.
Группа - это микромодель общественных реакций на поведение индивидуума. Каждый участник «создает» свое привычное жизненное пространство отношений с другими людьми. Увидев и осознав их ограниченность и неэффективность, можно попытаться менять свой способ взаимоотношений.
В нормально развивающейся группе, за что, конечно, ответственен ведущий группы, можно не только всесторонне увидеть себя, моделировать свое поведение «здесь и теперь», но, что очень важно, получить поддержку при опробовании новых способов поведения. Группа предполагает живой обмен опытом создания и решения проблем.

В процессе обучения по дисциплине студенты выполняют РГР на следующую тему: С помощью алгоритма Эль-Гамаля на эллиптических кривых зашифровать сообщение.
Параметры кривой, генератор множества точек, секретный ключ и случайное число берутся по варианту.
Контрольные вопросы к РГР:
1)К какому классу шифров относится шифр Эль-Гамаля на ЭК?
2)Каким ключом шифруется сообщение в системе Эль-Гамаля?
3)Какую проблему нужно решить криптоаналитику для вскрытия схемы Эль-Гамаля на ЭК?
4)Почему для шифрования в схеме Эль-Гамаля каждый раз должно использоваться новое значение k?
5)В чем разница между классической схемой Эль-Гамаля и той же схемой, основанной на эллиптических кривых?

При подготовке к практическим занятиям студенты анализируют поставленные преподавателем задачи и проблемы и находят пути к их разрешению с использованием инструментальных средств офисных и специализированных информационных технологий, учебно-методической литературы, электронных изданий, глобальной сети Интернет и тренинго-тестирующих комплексов.

Рекомендации по подготовке к зачету с оценкой.
При подготовке необходимо ориентироваться на конспекты лекций (при наличии лекционного курса по дисциплине), рабочую программу дисциплины, нормативную, учебную и рекомендуемую литературу. Основное в подготовке к сдаче - это повторение всего материала дисциплины, по которому необходимо сдавать зачет с оценкой. При подготовке к сдаче студент весь объем работы должен распределять равномерно по дням, отведенным для подготовки к зачету с оценкой, контролировать каждый день выполнение намеченной работы. В период подготовки студент вновь обращается к уже изученному (пройденному) учебному материалу.

Обеспечение обучающихся инвалидов и лиц с ограниченными возможностями здоровья печатными и электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производиться с учетом того, чтобы предоставлять этот материал в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифло-информационных устройств.
Для освоения дисциплины будут использованы лекционные аудитории, оснащенные досками для письма, мультимедийное оборудование: проектор, проекционный экран. Для проведения семинарских (практических) занятий - мультимедийное оборудование: проектор, проекционный экран.
Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего и специального назначения:
- лекционная аудитория: мультимедийное оборудование, источники питания для индивидуальных технических средств;
- учебная аудитория для практических занятий (семинаров): мультимедийное оборудование;
- аудитория для лабораторных занятий и самостоятельной работы: стандартные рабочие места с персональными компьютерами.
В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусмотрено соответствующее количество мест для обучающихся с учетом ограничений их здоровья.
Для обучающихся инвалидов и лиц с ограниченными возможностями здоровья предусмотрено обслуживание по межбиблиотечному абонементу (МБА) с Хабаровской краевой специализированной библиотекой для слепых. По запросу пользователей НТБ инвалидов по зрению, осуществляется информационно-библиотечное обслуживание, доставка и выдача для работы в читальном зале книг в специализированных форматах для слепых.

Проведение учебного процесса может быть организовано с использованием ЭИОС университета и в цифровой среде (группы в социальных сетях, электронная почта, видеоконференцсвязь и др. платформы). Учебные занятия с применением дистанционных образовательных технологий (ДОТ) проходят в соответствии с утвержденным расписанием. Текущий

контроль и промежуточная аттестация обучающихся проводится с применением ДОТ.