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

УТВЕРЖДАЮ

Зав.кафедрой
(к902) Высшая математика

Виноградова Полина
Витальевна

17.05.2023

РАБОЧАЯ ПРОГРАММА

дисциплины **Эллиптические системы в криптографии**

для направления подготовки 01.03.02 Прикладная математика и информатика

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

Обсуждена на заседании кафедры: (к902) Высшая математика

Протокол от 17.05.2023г. № 5

Обсуждена на заседании методической комиссии по родственным направлениям и специальностям: Протокол

г. Хабаровск
2024 г.

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

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2027 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры (к902) Высшая математика

Протокол от __ _____ 2027 г. № __
Зав. кафедрой Виноградова Полина Витальевна

Визирование РПД для исполнения в очередном учебном году

Председатель МК РНС

__ _____ 2028 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры (к902) Высшая математика

Протокол от __ _____ 2028 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 10.01.2018 № 9

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
в том числе:
контактная работа 52
самостоятельная работа 92

Виды контроля в семестрах:
зачёты (семестр) 6

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. 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.36
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Алгебра и геометрия
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Распознавание образов
2.2.2	Преддипломная практика

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

ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Знать:

– Методы решения задач профессиональной деятельности, с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Уметь:

– проектировать информационные системы на основе стандартов и исходных требований к проектированию и разработке информационных систем

Владеть:

– Методами решения задач профессиональной деятельности, с использованием существующих ин-формационно-коммуникационных технологий и с учетом основных требований информационной безопасности
– навыками построения пользовательских интерфейсов интегрированных систем;

ПК-3: Способностью проектировать элементы систем управления, применять современные инструментальные средства и технологии программирования на основе профессиональной подготовки, обеспечивающие решение задач системного анализа и управления

Знать:

– основные положения теории защиты информации и математические методы преобразования информации с целю ее защиты;
– математические методы, основанные на алгебраических структурах; алгоритмы защиты информации;
– основные алгоритмы математического обеспечения защиты информации

Уметь:

– применять методы систематизации и обработки данных.
– анализировать и оценивать угрозы информационной безопасности объекта;
– применять современный математический аппарат при разработке алгоритмов защиты;

Владеть:

– навыками использования математического аппарата в задачах моделирования защиты информации;
– математическими методами и средствами разработки алгоритмов преобразования информации

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	Математические основы классической криптографии /Лек/	6	4	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1Л3.1 Э1 Э2	2	
1.2	Математический аппарат, связанный с эллиптическими кривыми и конечными полями /Лек/	6	6	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2	6	

1.3	Протоколы криптосистем на эллиптические кривых /Лек/	6	2	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2	2	
1.4	Механизм выбора эллиптической кривой и точки на ней. /Лек/	6	2	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2	2	Работа в малых группах
1.5	Кодировка сообщений точками эллиптической кривой. /Лек/	6	2	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1Л3.1 Э1 Э2	0	
	Раздел 2. Практика						
2.1	Основные алгоритмы теории чисел. Анализ их быстродействия /Пр/	6	4	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1 Э2	0	
2.2	Мультипликативно обратное для разных модулей. /Пр/	6	4	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1 Э2	0	
2.3	Сложение и умножение в группе точек ЭК /Пр/	6	4	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.4	Алгоритмы вычисления количества точек на ЭК /Пр/	6	4	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.5	Алгоритмы кодировки сообщений точками эллиптической кривой. Шифр Эль-Гамаля /Пр/	6	4	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.6	Обмен ключами с использованием ЭК. Протокол Диффи-Хеллмана /Пр/	6	4	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.7	ЭЦП по ГОСТ 34.11-2018 /Пр/	6	4	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.8	Анализ криптографических алгоритмов на ЭК /Пр/	6	4	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Э1 Э2	2	Работа в малых группах
2.9	Изучение литературы /Ср/	6	58	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3Л2.1 Л2.2Л3.1 Л3.2 Э1	0	
2.10	Подготовка к практическим занятиям /Ср/	6	26	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э2	0	
2.11	Подготовка к зачету /Ср/	6	8	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2	0	
	Раздел 3. Зачет						

3.1	Зачет /Зачёт/	6	0	ПК-3 ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2	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., 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
Л1.3	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
Л1.4	Авдеева М. О.	Алгебра и аналитическая геометрия: учебное пособие	Хабаровск: Изд-во ДВГУПС, 2023,

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

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Яковлев В. В., Корниенко А. А.	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учеб. для вузов жд тр-та	Москва: УМК МПС России, 2002,
Л2.2	Аграновский А.В., Хади Р.А.	Практическая криптография	Москва: СОЛОН-Пресс, 2009, http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=13653

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	Трофимович П.Н., Виноградова П.В.	Организация и контроль самостоятельной работы студентов направлений подготовки 01.03.02, 01.04.02 "Прикладная математика и информатика": метод. рекомендации	Хабаровск: Изд-во ДВГУПС, 2017,

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

Э1	учер, Н. А. Краевые задачи для эллиптических систем уравнений на плоскости : учебное пособие : [16+] / Н. А. Кучер. – Кемерово : Кемеровский государственный университет, 2009. – 94 с.	https://biblioclub.ru/index.php?page=book&id=232683
Э2	Кучер, Н. А. Нелинейные краевые задачи на плоскости : учебное пособие / Н. А. Кучер, О. В. Малышенко. – Кемерово : Кемеровский государственный университет, 2012. – 116 с.	https://biblioclub.ru/index.php?page=book&id=232684

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
Mathcad Education - University Edition - Математический пакет, контракт 410
Lazarus, свободно распространяемое ПО
Free Conference Call (свободная лицензия)
Zoom (свободная лицензия)
АСТ тест - Комплекс программ для создания банков тестовых заданий, организации и проведения сеансов тестирования, лиц.АСТ.РМ.А096.Л08018.04, дог.372
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
1204	Учебная аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	комплект учебной мебели, доска.
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.
1201	Учебная аудитория для проведения практических занятий и лекций.	комплект учебной мебели, 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 в расчет надо брать 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.

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.

Методические указания по подготовке к лекциям, практическим занятиям, подготовке к зачету даны в пособии "Организация и контроль самостоятельной работы студентов", приведенном в списке литературы.

Рекомендации по подготовке к практическим занятиям
Студентам рекомендуется ознакомиться с теоретическим материалом по конспектам лекций, учебных пособий, книг и открытых информационных источников, рекомендованных преподавателем по соответствующим разделам для подготовки к занятию. Необходимо проработать материал, представленный в примерах на занятиях, выполнить домашнее задание.
При необходимости посетить консультации.

При подготовке к зачету студент должен повторить весь теоретический и практический материал курса. При сдаче зачета разрешается пользоваться справочной литературой.

Оценочные материалы при формировании рабочих программ дисциплин (модулей)

Направление: 01.03.02 Прикладная математика и информатика

Направленность (профиль): Системное программирование и компьютерные науки

Дисциплина: Эллиптические системы в криптографии

Формируемые компетенции:

1. Описание показателей, критериев и шкал оценивания компетенций.

Показатели и критерии оценивания компетенций

Объект оценки	Уровни сформированности компетенций	Критерий оценивания результатов обучения
Обучающийся	Низкий уровень Пороговый уровень Повышенный уровень Высокий уровень	Уровень результатов обучения не ниже порогового

Шкалы оценивания компетенций при сдаче зачета

Достигнутый уровень результата обучения	Характеристика уровня сформированности компетенций	Шкала оценивания
Пороговый уровень	Обучающийся: - обнаружил на зачете всесторонние, систематические и глубокие знания учебно-программного материала; - допустил небольшие упущения в ответах на вопросы, существенным образом не снижающие их качество; - допустил существенное упущение в ответе на один из вопросов, которое за тем было устранено студентом с помощью уточняющих вопросов; - допустил существенное упущение в ответах на вопросы, часть из которых была устранена студентом с помощью уточняющих вопросов	Зачтено
Низкий уровень	Обучающийся: - допустил существенные упущения при ответах на все вопросы преподавателя; - обнаружил пробелы более чем 50% в знаниях основного учебно-программного материала	Не зачтено

Описание шкал оценивания

Компетенции обучающегося оценивается следующим образом:

Планируемый уровень результатов освоения	Содержание шкалы оценивания достигнутого уровня результата обучения			
	Неудовлетворительн	Удовлетворительно	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено

Знать	Неспособность обучающегося самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся способен самостоятельно продемонстриро-вать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения.	Обучающийся демонстрирует способность к самостоятельному применению знаний при решении заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной	Обучающийся демонстрирует способность к самостоятельно-му применению знаний в выборе способа решения неизвестных или нестандартных заданий и при консультативной поддержке в части междисциплинарных
Уметь	Отсутствие у обучающегося самостоятельности в применении умений по использованию методов освоения учебной дисциплины.	Обучающийся демонстрирует самостоятельность в применении умений решения учебных заданий в полном соответствии с образцом, данным преподавателем.	Обучающийся продемонстрирует самостоятельное применение умений решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение умений решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.
Владеть	Неспособность самостоятельно проявить навык решения поставленной задачи по стандартному образцу повторно.	Обучающийся демонстрирует самостоятельность в применении навыка по заданиям, решение которых было показано преподавателем.	Обучающийся демонстрирует самостоятельное применение навыка решения заданий, аналогичных тем, которые представлял преподаватель, и при его консультативной поддержке в части современных проблем.	Обучающийся демонстрирует самостоятельное применение навыка решения неизвестных или нестандартных заданий и при консультативной поддержке преподавателя в части междисциплинарных связей.

2. Перечень вопросов и задач к экзаменам, зачетам, курсовому проектированию, лабораторным занятиям. Образец экзаменационного билета

1. Алгебраические структуры. Полугруппы. Моноиды. Группы. Кольца. Поля.
2. Делимость и деление с остатком в кольце целых чисел.
3. Наибольший общий делитель и его свойства. Алгоритм Евклида.
4. Простые и составные числа. Теорема Евклида. Основная теорема арифметики.
5. Сравнения. Кольца классов вычетов по простому и составному модулю. Полная и приведенная системы вычетов.
6. Функция Эйлера. Теоремы Ферма и Эйлера.
7. История изучения эллиптических кривых. Эллиптические кривые для криптографических алгоритмов и протоколов в ГОСТах и стандартах РФ.
8. Алгебраические кривые над полями. Приводимость алгебраических кривых.
9. Найти все F_5-точки кривой y^2=x^3+2.
10. Найти все точки эллиптической кривой E7(2,6)
11. Особые точки кубической кривой.
12. Построить кривую x^3-x^2+y^2=0 и найти ее касательные в точке (0, 0).
13. Построить действительную часть кривой x^3+x^2+y^2=0 и найти ее касательные в точке (0, 0).
14. Однородный полином. Равенство полных степеней полинома и однородного ему. Эквивалентность троек чисел (элементов) поля.
15. Геометрическое построение проективной плоскости.
16. Плоскость Фано (построение точек и прямых).
17. Найти точки проективной плоскости над полем Галуа F_3={0,1,2}.

18. Сложение точек на прямых, окружностях и других кривых второго порядка (на плоскости) как групповая операция.

19. Найти координаты суммы двух точек (x_1,y_1) и (x_2,y_2) параболы y=x^2 с фиксированной точкой E=(0,0).

20. Закон сложения точек плоской кубической кривой. Количество точек пересечения прямой и кубической кривой.

21. Найти координаты суммы двух точек кубической параболы y=x^3 с фиксированной точкой E=(0,0).

22. Определение эллиптической кривой над полем. Характеристика поля. Канонические уравнения эллиптической кривой.

23. Теорема о девяти точках кубической кривой.

24. Ассоциативность операции сложения точек кубической кривой.

25. Формулы координат суммы точек с различными абсциссами кривой Вейерштрасса.

26. Формулы удвоения точек кривой Вейерштрасса.

27. Бесконечно удаленная точка кривой Вейерштрасса. Правила сложения точек кривой Вейерштрасса.

28. Кратность точек кубической кривой. Неособенные кубические кривые. Точки перегиба неособенной кривой. Эллиптические кривые.

29. Доказать, что точка бесконечности кривой Вейерштрасса - точка перегиба.

30. Множество точек перегиба кривой Вейерштрасса и их свойства.

31. Приведение уравнения эллиптической кривой с заданной точкой перегиба к виду Вейерштрасса.

32. Приведение уравнения эллиптической кривой с заданной рациональной точкой к виду Вейерштрасса.

33. Точки кручения. Ранг эллиптической кривой. Теорема Морделла.

34. Найти порядок точки p=(2,3). на эллиптической кривой y^2=x^3+1.

35. Эллиптический вариант криптосистемы Месси-Омуры

36. Криптосистема Эль-Гомаля и задача дискретного логарифмирования на эллиптической кривой.

37. Аналог протокола Джеффи-Хеллмана на эллиптической кривой

38. Алгоритм Тонелли-Шенкса.

39. Задача кодирования открытого текста точками эллиптической кривой.

40. Факторизация чисел с помощью эллиптических кривых.

3. Тестовые задания. Оценка по результатам тестирования.

Задание 1 (ПК-3, ОПК-4)

Выберите правильный вариант ответа.

Условие задания: Выбрать правильное определение

 Неособая кривая третьего порядка над полем называется эллиптической кривой над этим полем, если на ней есть хотя бы одна точка.

 Кривая третьего порядка над полем называется эллиптической кривой над этим полем, если на ней есть хотя бы одна особая точка.

 Особая кривая третьего порядка над полем называется эллиптической кривой над этим полем, если на ней есть хотя бы одна точка.

Задание 2 (ПК-3, ОПК-4)

Установить историческую последовательность математиков, изучавших эллиптические функции:

1: Нильс Хенрик Абель

2: Карл Густав Якоби

3: Карл Вейерштрасс

Задание 3 (ПК-3, ОПК-4)

Установите соответствие между полем с определнной характеристикой и видом уравнения эллиптической кривой в нем

поле характеристики, отличной от 2 и 3	y2=x3+ax+b;
поле характеристики 3	y2+ay=x3+bx+c;
поле характеристики 2 (суперсингулярная кривая)	y2+ay=x3+bx+c;
поле характеристики 2 (несупесингулярная кривая)	y2+axy=x3+bx2+c;
	y2+ay=x2+bx+c

Задание 4 (ПК-3, ОПК-4)

Вставить число
Порядок группы точек кривой E7(2,6) равен ____ .
Правильный вариант ответа: 11;

Задание 5 (ПК-3, ОПК-4)
Вставить пропущенный термин
Точка P будет называться ____ , если кратные ей точки образуют все множество точек эллиптической кривой.
Правильные варианты ответа: генератором группы; генеретор группы.

Полный комплект тестовых заданий в корпоративной тестовой оболочке АСТ размещен на сервере УИТ ДВГУПС, а также на сайте Университета в разделе СДО ДВГУПС (образовательная среда в личном кабинете преподавателя).

Соответствие между бальной системой и системой оценивания по результатам тестирования устанавливается посредством следующей таблицы:

Объект оценки	Показатели оценивания результатов обучения	Оценка	Уровень результатов обучения
Обучающийся	60 баллов и менее	«Неудовлетворительно»	Низкий уровень
	74 – 61 баллов	«Удовлетворительно»	Пороговый уровень
	84 – 75 баллов	«Хорошо»	Повышенный уровень
	100 – 85 баллов	«Отлично»	Высокий уровень

4. Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета, курсового проектирования.

Оценка ответа обучающегося на вопросы, задачу (задание) экзаменационного билета, зачета

Элементы оценивания	Содержание шкалы оценивания			
	Неудовлетворительн	Удовлетворитель	Хорошо	Отлично
	Не зачтено	Зачтено	Зачтено	Зачтено
Соответствие ответов формулировкам вопросов (заданий)	Полное несоответствие по всем вопросам.	Значительные погрешности.	Незначительные погрешности.	Полное соответствие.
Структура, последовательность и логика ответа. Умение четко, понятно, грамотно и свободно излагать свои мысли	Полное несоответствие критерию.	Значительное несоответствие критерию.	Незначительное несоответствие критерию.	Соответствие критерию при ответе на все вопросы.
Знание нормативных, правовых документов и специальной литературы	Полное незнание нормативной и правовой базы и специальной литературы	Имеют место существенные упущения (незнание большей части из документов и специальной литературы по названию, содержанию и т.д.).	Имеют место несущественные упущения и незнание отдельных (единичных) работ из числа обязательной литературы.	Полное соответствие данному критерию ответов на все вопросы.

Умение увязывать теорию с практикой, в том числе в области профессиональной работы	Умение связать теорию с практикой работы не проявляется.	Умение связать вопросы теории и практики проявляется редко.	Умение связать вопросы теории и практики в основном проявляется.	Полное соответствие данному критерию. Способность интегрировать знания и привлекать сведения из различных научных сфер.
Качество ответов на дополнительные вопросы	На все дополнительные вопросы преподавателя даны неверные ответы.	Ответы на большую часть дополнительных вопросов преподавателя даны неверно.	. Даны неполные ответы на дополнительные вопросы преподавателя. 2. Дан один неверный ответ на дополнительные вопросы преподавателя.	Даны верные ответы на все дополнительные вопросы преподавателя.

Примечание: итоговая оценка формируется как средняя арифметическая результатов элементов оценивания.