УТВЕРЖДЕНО

решением Ученого совета факультета математики,
информационных и авиационных технологий
от «21» 05 2024г., протокол № 5/24
Председатель _____ Волков М.А.
«21» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Методы алгебраической геометрии в криптографии**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	5

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Рацеев Сергей Михайлович	Кафедра информационной безопасности и теории управления	Профессор,Доктор физико-математических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

- ознакомление студентов с основными понятиями алгебраической геометрии;
- развитие навыка построения криптографических протоколов на эллиптических кривых.

Задачи освоения дисциплины:

- овладение основными идеями и методами построения криптографических систем на основе эллиптических кривых;
- формирование навыков грамотного применения теоретических основ криптографии в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Методы алгебраической геометрии в криптографии» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-3.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Теория кодирования, сжатия и восстановления информации, Методы и средства криптографической защиты информации, Теория псевдослучайных генераторов, Вычислительные методы в алгебре и теории чисел, Математическая логика и теория алгоритмов, Дифференциальные уравнения, Алгебра и геометрия, Теория вероятностей, Математический анализ, Научно-исследовательская работа, Численные методы, Ознакомительная практика, Методы алгебраической геометрии в криптографии, Избранные вопросы математического анализа, Проектная деятельность, Подготовка к сдаче и сдача государственного экзамена.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	**Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций**
ОПК-3 Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;	**знать**: протоколы эллиптической криптографии; методы приложения конечных полей в криптографии; протоколы электронной подписи на основе эллиптических кривых **уметь**: решать задачи на алгебраические многообразия; разрабатывать быстрые вычислительные алгоритмы для криптографических приложений **владеть**:

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	криптографической терминологией

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 7 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 252 часа

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)		
	Всего по плану	В т.ч. по семестрам	
		9	10
1	2	3	4
Контактная работа обучающихся с преподавателем в соответствии с УП	148	108	40
Аудиторные занятия:	148	108	40
Лекции	56	36	20
Семинары и практические занятия	36	36	0
Лабораторные работы, практикумы	56	36	20
Самостоятельная работа	68	36	32
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование	Тестирование	
Курсовая работа	-	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачет, Экзамен (18)	Зачет	Экзамен
Всего часов по дисциплине	252	144	108

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Раздел 1. Алгебраическая основа							
Тема 1.1. Группы. Кольца.	18	4	4	0	0	10	Вопросы к Экзамену, Тестирование
Тема 1.2. Поля.	28	10	8	8	0	2	Вопросы к Экзамену, Тестирование
Тема 1.3. Применение конечных полей в криптографии.	32	10	10	8	2	4	Вопросы к Экзамену, Тестирование
Раздел 2. Элементы алгебраической геометрии							
Тема 2.1. Аффинные алгебраические многообразия.	8	4	2	0	0	2	Вопросы к Экзамену, Тестирование
Тема 2.2. Проективная плоскость.	8	4	2	0	0	2	Вопросы к Экзамену, Тестирование
Тема 2.3. Эллиптические кривые.	40	10	10	16	16	4	Вопросы к Экзамену, Тестирование
Раздел 3. Протоколы на эллиптических кривых							
Тема 3.1. Выбор точки и размещение данных.	4	2	0	0	0	2	Вопросы к Экзамену, Тестирование
Тема 3.2. Криптосистемы на эллиптических кривых.	38	10	0	24	0	4	Вопросы к Экзамену, Тестирование

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Тема 3.3. Дискретное логарифмирование на эллиптической кривой.	40	2	0	0	0	38	Вопросы к Экзамену, Тестирование
Итого подлежит изучению	216	56	36	56	18	68	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Алгебраическая основа

Тема 1.1. Группы. Кольца.

Алгебраические операции. Группы. Основные свойства группы. Подгруппы. Эквивалентные условия подгруппы. Циклическая группа. Свойства циклических групп. Смежные классы. Индекс подгруппы. Теорема Лагранжа. Нормальная подгруппа. Эквивалентные условия нормальной подгруппы. Фактор-группа. Морфизмы групп. Ядро и образ гомоморфизма. Теорема о гомоморфизме групп. Кольца. Мультипликативная группа кольца. Подкольца. Критерий подкольца. Идеал кольца. Фактор-кольцо. Кольца вычетов. Морфизмы колец. Ядро и образ гомоморфизма. Теорема о гомоморфизме колец. Кольца главных идеалов. Китайская теорема об остатках для идеалов колец. Разложение кольца вычетов в прямую сумму примарных колец.

Тема 1.2. Поля.

Поле. Подполе. Простое поле. Характеристика поля. Простые идеалы. Поле частных. Расширение поля. Теорема о башне расширений. Конечные расширения. Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента, некоторые его свойства. Строение расширения поля, полученное присоединением алгебраического элемента. Поля разложения многочлена. Конечные поля. Теорема о числе элементов конечного поля. Цикличность мультипликативной группы конечного поля. Образующие элементы конечного поля. Неприводимые многочлены над конечными полями. Автоморфизм Фробениуса. Совершенные поля. Трансцендентные расширения полей.

Тема 1.3. Применение конечных полей в криптографии.

Блочный шифр «Кузнечик» из ГОСТ Р 34.12-2015. Шифр AES. Рюкзачная криптосистема Шора-

Ривеста на основе конечных полей. Построение ортогональных таблиц над конечными полями. Совершенные шифры на основе ортогональных таблиц.

Раздел 2. Элементы алгебраической геометрии

Тема 2.1. Аффинные алгебраические многообразия.

Аффинные алгебраические многообразия. Теорема Гильберта. Примеры алгебраических многообразий и их идеалов. Неприводимые алгебраические многообразия. Гиперповерхность.

Тема 2.2. Проективная плоскость.

Проективная прямая. Проективная плоскость. Проективные и аффинные кривые, связь между ними. Пифагоровы тройки. Рациональные кривые.

Тема 2.3. Эллиптические кривые.

Плоские аффинные кубические кривые. Особые и неособые точки. Определение эллиптической кривой. Нормальная форма Вейерштрасса. Дискриминант и j-инвариант. Точки перегиба кубических кривых. Закон сложения точек эллиптической кривой. Касательные и точки перегиба кубической кривой. Группа неособых точек кубики. Точки конечного порядка. Эллиптические кривые над числовыми полями. Теорема Мазура. Теорема Морделла-Вейля. Отображения алгебраических кривых. Дивизоры на алгебраических кривых. Эллиптические кривые над конечными полями. Гиперэллиптические кривые.

Раздел 3. Протоколы на эллиптических кривых

Тема 3.1. Выбор точки и размещение данных.

Выбор точки эллиптической кривой. Размещение данных на эллиптической кривой. Определение порядка точки эллиптической кривой и нахождение образующего элемента группы точек эллиптической кривой.

Тема 3.2. Криптосистемы на эллиптических кривых.

Модификация системы Диффи-Хеллмана на эллиптических кривых. Вероятностное щифрование на основе эллиптических кривых, модификация шифра Эль-Гаамаля. Модификация протокола Месси-Омуры на эллиптических кривых. Модификация протокола Шнорра на эллиптических кривых. Модификация трехпроходного протокола Шнорра на эллиптических кривых. Модификация протокола Окамото на эллиптических кривых. Модификация семейства протоколов MTI на эллиптических кривых. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых. Модификация протокола голосования на эллиптических кривых. Пятипроходный протокол идентификации на основе изоморфизма графов с использованием эллиптических кривых. Модификация схемы Фельдмана-Шамира на эллиптических кривых. Модификация схемы Педерсона-Шамира на

эллиптических кривых. Электронная подпись ГОСТ Р 34.10-2012. Электронная подпись ECDSA.

Тема 3.3. Дискретное логарифмирование на эллиптической кривой.

Критерий простоты, использующий эллиптические кривые. Разложение на множители при помощи эллиптических кривых. Универсальные методы логарифмирования. Гельфонда-Шенкса. Метод Полларда. Метод встречи на случайном дереве. Логарифмирование с использованием функции Вейля. Требования к эллиптической кривой.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Алгебраическая основа

Тема 1.1. Группы. Кольца.

Вопросы к теме:

Очная форма

Группы. Подгруппы. Эквивалентные условия подгруппы. Циклическая группа. Свойства циклических групп. Смежные классы. Индекс подгруппы. Теорема Лагранжа. Нормальная подгруппа. Эквивалентные условия нормальной подгруппы. Фактор-группа. Морфизмы групп. Ядро и образ гомоморфизма. Кольца. Мультипликативная группа кольца. Подкольца. Критерий подкольца. Идеал кольца. Фактор-кольцо. Кольца вычетов. Морфизмы колец. Ядро и образ гомоморфизма. Китайская теорема об остатках для идеалов колец. Разложение кольца вычетов в прямую сумму примарных колец.

Тема 1.2. Поля.

Вопросы к теме:

Очная форма

Поле. Подполе. Простое поле. Характеристика поля. Простые идеалы. Поле частных. Расширение поля. Конечные расширения. Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента. Строение расширения поля, полученное присоединением алгебраического элемента. Поля разложения многочлена. Конечные поля. Образующие элементы конечного поля. Неприводимые многочлены над конечными полями.

Тема 1.3. Применение конечных полей в криптографии.

Вопросы к теме:

Очная форма

Блочный шифр «Кузнечик» из ГОСТ Р 34.12-2015. Рюкзачная криптосистема Шора-Ривеста на основе конечных полей. Построение ортогональных таблиц над конечными полями. Совершенные шифры на основе ортогональных таблиц.

Раздел 2. Элементы алгебраической геометрии

Тема 2.1. Аффинные алгебраические многообразия.

Вопросы к теме:

Очная форма

Аффинные алгебраические многообразия. Примеры алгебраических многообразий и их идеалов. Неприводимые алгебраические многообразия.

Тема 2.2. Проективная плоскость.

Вопросы к теме:

Очная форма

Проективная прямая. Проективная плоскость. Проективные и аффинные кривые, связь между ними. Рациональные кривые.

Тема 2.3. Эллиптические кривые.

Вопросы к теме:

Очная форма

Плоские аффинные кубические кривые. Особые и неособые точки. Закон сложения точек эллиптической кривой. Точки конечного порядка. Эллиптические кривые над числовыми полями. Эллиптические кривые над конечными полями. Гиперэллиптические кривые.

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Реализация конечных полей
Цели: Ознакомиться с методами построения конечных полей.
Содержание: Написать программу, реализующую арифметику конечного поля по неприводимому многочлену.
Результаты: Основное внимание должно быть уделено освоению методов построения конечных полей.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Реализация эллиптических кривых
Цели: Ознакомиться с групповым законом эллиптической кривой.

Содержание: Написать программу, реализующую арифметику аддитивной абелевой группы на эллиптической кривой.
Результаты: Основное внимание должно быть уделено освоению аддитивной группы эллиптической кривой.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Шифр Кузнечик
Цели: Ознакомиться с методами симметричного шифрования с использованием конечных полей.
Содержание: Написать программу, реализующую шифр Кузнечик из ГОСТ Р 34.12-2015.
Результаты: Основное внимание должно быть уделено освоению методов применения конечных полей при построении криптосистем.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Ознакомиться с протоколами на эллиптических кривых.
Цели: Протокол Диффи-Хеллмана для эллиптических кривых.
Содержание: Написать программу, с помощью которой реализуема адаптация протокола Диффи-Хеллмана для эллиптических кривых.
Результаты: Основное внимание должно быть уделено освоению методов построений протоколов на эллиптических кривых.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Электронная подпись ГОСТ Р 34.10-2012.
Цели: Ознакомиться с протоколами на эллиптических кривых.
Содержание: Написать программу, реализующую электронную подпись ГОСТ Р 34.10-2012.
Результаты: Основное внимание должно быть уделено освоению методов построений протоколов на эллиптических кривых.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Данный вид работы не предусмотрен УП.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ, ЗАЧЕТУ

Вопросы к экзамену

1. Китайская теорема об остатках для идеалов колец. Разложение кольца вычетов в прямую сумму примарных колец.
2. Конечные поля. Построение конечного поля.
3. Образующие элементы конечного поля.
4. Блочный шифр «Кузнечик» из ГОСТ Р 34.12-2015.
5. Рюкзачная криптосистема Шора-Ривеста на основе конечных полей.
6. Аффинные алгебраические многообразия.
7. Проективная плоскость.
8. Эллиптические кривые: определение, общая форма Вейерштрасса эллиптической кривой.
9. Сложение точек эллиптической кривой над полем R.
10. Сложение точек эллиптической кривой над конечным полем.

11. Модификация системы Диффи-Хеллмана на эллиптических кривых.
12. Вероятностное шифрование на основе эллиптических кривых, модификация шифра Эль-Гамаля.
13. Модификация протокола Месси-Омуры на эллиптических кривых.
14. Модификация схемы разделения секрета Педерсона-Шамира на эллиптических кривых.
15. Модификация протокола аутентификации Шнорра на эллиптических кривых.
16. Модификация трехпроходного протокола аутентификации Шнорра на эллиптических кривых.
17. Модификация протокола аутентифкации Окамото на эллиптических кривых.
18. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых.
19. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамаля с использованием эллиптических кривых.
20. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых.
21. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых.
22. Электронная подпись ГОСТ Р 34.10-2012.

Вопросы к зачету

1. Алгебраические операции. Группы. Основные свойства группы.

2. Подгруппы. Эквивалентные условия подгруппы.

3. Циклическая группа. Свойства циклических групп.

4. Морфизмы групп. Ядро и образ гомоморфизма. Теорема о гомоморфизме групп.

5. Кольца. Мультипликативная группа кольца. Подкольца. Критерий подкольца.

6. Идеал кольца. Фактор-кольцо. Кольца вычетов.

7. Морфизмы колец. Ядро и образ гомоморфизма. Теорема о гомоморфизме колец. Кольца главных идеалов.

8. Поле: определение и основные свойства. Подполе. Критерий подполя. Критерий конечного подполя.

9. Простые поля. Характеристика поля.

10. Расширение поля. Теорема о башне полей.

11. Алгебраические и трансцендентные элементы поля. Простые расширения полей. Теорема о классификации простых расширений полей.

12. Конечные поля. Построение конечного поля.

13. Образующие элементы конечного поля.

14. Неприводимые многочлены над конечными полями.

15. Блочный шифр «Кузнечик» из ГОСТ Р 34.12-2015.

16. Рюкзачная криптосистема Шора-Ривеста на основе конечных полей.

17. Аффинные алгебраические многообразия. Примеры алгебраических многообразий и их идеалов.

18. Неприводимые аффинные многообразия.

19. Проективная плоскость.

20. Эллиптические кривые: определение, общая форма Вейерштрасса эллиптической кривой.

21. Сложение точек эллиптической кривой над полем R.

22. Сложение точек эллиптической кривой над конечным полем.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Алгебраическая основа			
Тема 1.1. Группы. Кольца.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	10	Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Тема 1.2. Поля.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 1.3. Применение конечных полей в криптографии.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Раздел 2. Элементы алгебраической геометрии			
Тема 2.1. Аффинные алгебраические многообразия.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 2.2. Проективная плоскость.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 2.3. Эллиптические кривые.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Раздел 3. Протоколы на эллиптических кривых			
Тема 3.1. Выбор точки и размещение данных.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 3.2. Криптосистемы на эллиптических кривых.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 3.3. Дискретное логарифмирование на эллиптической кривой.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	38	Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Рацеев Сергей Михайлович. Математические методы защиты информации : учебное пособие для вузов / С.М. Рацеев. - Санкт-Петербург : Лань, 2023. - 543 с. - (Высшее образование). - ISBN 978-5-8114-8589-5 (в пер.). / .— ISBN 1_258181

2. Черемушкин Александр Васильевич. Криптографические протоколы. Основные свойства и уязвимости : учеб. пособие для вузов по спец. "Компьютер. безопасность" / А.В. Черемушкин. - Москва : Академия, 2009. - 272 с. : ил. - (Высшее профессиональное образование) (Информационная безопасность). - Библиогр.: с. 264-270. - ISBN 978-5-7695-5748-4 (в пер.). / .— ISBN 1_182853

дополнительная

1. Рацеев Сергей Михайлович. Математические методы защиты информации и их основы. Сборник задач : учебное пособие для вузов / С.М. Рацеев. - Санкт-Петербург : Лань, 2023. - 136 с. - (Высшее образование). - Библиогр.: с. 135-136. - ISBN 978-5-507-45197-5 (в пер.). / .— ISBN 1_258183

2. Рябко Б.Я. Криптографические методы защиты информации : учебное пособие / Б.Я. Рябко, А.Н. Фионов ; Рябко Б.Я.; Фионов А.Н. - Москва : Горячая линия - Телеком, 2012. - 229 с. - URL: https://www.studentlibrary.ru/book/ISBN9785991202862.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-9912-0286-2. / .— ISBN 0_242519

учебно-методическая

1. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Методы алгебраической геометрии в криптографии» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев. - 2022. - 9 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13334. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_475959.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Visual studio code

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Доктор физико-математических наук, Доцент	Рацеев Сергей Михайлович
	Должность, ученая степень, звание	ФИО