УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от « 18 » 05 2021 г., протокол № 4/21
Председатель М.А. Волков
(подпись, расшифровка подписи)
« 18 » 05 2021 г.

РАБОЧАЯ ПРОГРАММА

Дисциплина	Методы алгебраической геометрии в криптографии
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	5

Специальность: 10.05.01 «Компьютерная безопасность»
код направления (специальности), полное наименование

Специализация: «Математические методы защиты информации»
полное наименование

Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: « 01 » 09 2021 г.

Программа актуализирована на заседании кафедры: протокол №____ от _____ 20_____ 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	ИБиТУ	профессор, д.ф-м.н, доцент

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой «Информационная безопасность и теория управления», реализующей дисциплину	Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
/ _____ / Андреев А.С. / *(подпись) (Ф.И.О.)* « 12 » 05 2021 г.	/ _____ / Андреев А.С. / *(подпись) (Ф.И.О.)* « 12 » 05 2021 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Курс «Методы алгебраической геометрии в криптографии» составляет одну из фундаментальных частей современной теоретической криптографии, без знания которых невозможна дальнейшая профессиональная подготовка в области современной защиты информации. При освоении данного курса у студентов формируются навыки грамотного применения теоретических основ криптографии в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

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 относится к обязательной части цикла Б1 образовательной программы и читается в 9-м и 10-м семестрах студентам специальности «Компьютерная безопасность» очной формы обучения.

Для успешного освоения дисциплины необходимы знания основных фактов из базовых курсов: «Математический анализ», «Алгебра», «Дискретная математика», «Информатика», «Методы и средства криптографической защиты информации».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: основные задачи и понятия криптографии; классификацию шифров по различным признакам; типы основных способов криптоанализа шифров; основные типы электронной подписи.

Дисциплина «Методы алгебраической геометрии в криптографии» является предшествующей для прохождения преддипломной практики и итоговой государственной аттестации.

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

Процесс изучения дисциплины «Методы алгебраической геометрии в криптографии» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-2.1 – Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	Знать: методы построения конечных полей; протоколы эллиптической криптографии; протоколы электронной подписи на основе эллиптических кривых; Уметь:

	решать задачи на алгебраические многообразия; разрабатывать быстрые вычислительные алгоритмы для криптографических приложений; Владеть: криптографической терминологией
ОПК-2.2 – Способен разрабатывать и анализировать математические модели механизмов защиты информации	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: криптографической терминологией

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего) 7**.**

4.2. Объем дисциплины по видам учебной работы:

Вид учебной работы	Количество часов (форма обучения - дневная)			
	Всего по плану	В т.ч. по семестрам		
		9	10	
Контактная работа обучающихся с преподавателем	120/120*	90/90*	30/30*	
Аудиторные занятия:				
• Лекции	56/56*	36/36*	20/20*	
• Практические и семинарские занятия	36/36*	36/36*		
• Лабораторные работы (лабораторный практикум)	28/28*	18/18*	10/10*	
Самостоятельная работа	96	54	42	
Экзамен	36		36	
Курсовая работа	+		+	
Всего часов по дисциплине	252	144	108	
Форма текущего контроля знаний и контроля самостоятельной работы		Лабораторные работы, проверка ре-	Лабораторные работы, проверка решения задач	

		шения задач		
Виды промежуточной аттестации (экзамен, зачет)		зачет	экзамен	
Общая трудоемкость в зач. ед.	7	4	3	

**В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения*

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	
Раздел 1. Алгебраическая основа							
1. Группы. Кольца.	16	4	4			8	Домашние задания
2. Поля.	40	10	8	4	2	18	Лабораторная работа. Домашние задания
3. Применение конечных полей в криптографии.	44	10	10	4	10	20	Лабораторная работа. Домашние задания
Раздел 2. Элементы алгебраической геометрии							
4. Аффинные алгебраические многообразия.	12	4	2			6	Домашние задания
5. Проективная плоскость.	12	4	2			6	Домашние задания
6. Эллиптические кривые.	38	10	10	8	12	10	Лабораторная работа. Домашние задания
Раздел 3. Протоколы на эллиптических кривых							
7. Выбор точки и размещение данных (10 сем).	4	2				2	
8. Криптосисте-	40	10		12	8	18	Лабораторная

мы на эллиптических кривых.							работа. Домашние задания
9.Дискретное логарифмирование на эллиптической кривой	10	2				8	
Экзамен	36						
ВСЕГО	252	56	36	28	32	96	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Раздел 1. Алгебраическая основа

Тема 1. Группы.

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 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 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 4. Аффинные алгебраические многообразия.

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

Тема 5. Проективная плоскость.

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

Тема 6. 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 по-

рядка. 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 7. 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 8. Криптосистемы на эллиптических кривых.

Модификация системы Диффи-Хеллмана на эллиптических кривых. Вероятностное шифрование 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 9. 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. Группы. Форма проведения – семинар.

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 2. Поля. Форма проведения – семинар.

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 3. Применение конечных полей в криптографии. Форма проведения – семинар.

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 4. Аффинные алгебраические многообразия. Форма проведения – семинар.
Аффинные алгебраические многообразия. Примеры алгебраических многообразий и их идеалов. Неприводимые алгебраические многообразия.
Тема 5. Проективная плоскость. Форма проведения – семинар.
Проективная прямая. Проективная плоскость. Проективные и аффинные кривые, связь между ними. Рациональные кривые.
Тема 6. Эллиптические кривые. Форма проведения – семинар.
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.

Раздел 3. Протоколы на эллиптических кривых
Тема 7. Выбор точки и размещение данных. Форма проведения – семинар.
Выбор точки эллиптической кривой. Размещение данных на эллиптической кривой. Определение порядка точки эллиптической кривой и нахождение образующего элемента группы точек эллиптической кривой.
Тема 8. Криптосистемы на эллиптических кривых. Форма проведения – семинар.
Модификация системы Диффи-Хеллмана на эллиптических кривых. Вероятностное шифрование 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 9. Дискретное логарифмирование на эллиптической кривой. Форма проведения – семинар.
Метод Гельфонда-Шенкса. Метод Полларда. Метод встречи на случайном дереве.

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Лабораторные работы проводятся в интерактивной форме, а именно, используются: диалоговое обучение, в ходе которого осуществляется взаимодействие между студентом и преподавателем, между самими студентами, группами студентов; элементы деловых игр, «мозговой штурм» или дискуссии по рассматриваемым вопросам.

Полные задания для лабораторных работ приводятся в методическом пособии:
Рацеев С.М. Лабораторный практикум по методам алгебраической геометрии в криптографии [Электронный ресурс] / С. М. Рацеев; УлГУ, ФМИАТ, Каф. информ. безопасности и теории управления. - Ульяновск : УлГУ, 2019.

Раздел 1. Алгебраическая основа
Тема 2. Поля.
Цель работы: ознакомиться с методами построения конечных полей.
Задание. Написать программу, реализующую арифметику конечного поля по неприводимому многочлену.
Методические указания: основное внимание должно быть уделено освоению методов построения конечных полей.
Тема 3. Применение конечных полей в криптографии.
Цель работы: ознакомиться с методами симметричного шифрования с использованием конечных полей.
Задание. Написать программу, реализующую шифр Кузнечик из ГОСТ Р 34.12-2015.
Методические указания: основное внимание должно быть уделено освоению методов применения конечных полей при построении криптосистем.

Раздел 2. Элементы алгебраической геометрии
Тема 6. Эллиптические кривые.
Цель работы: ознакомиться с групповым законом эллиптической кривой.
Задание. Написать программу, реализующую арифметику аддитивной абелевой группы на эллиптической кривой.
Методические указания: основное внимание должно быть уделено освоению аддитивной группы эллиптической кривой.
Тема 6. Эллиптические кривые.
Цель работы: ознакомиться с групповым законом эллиптической кривой.
Задание. Написать программу генерации точки, образующей группу порядка r на эллиптической кривой.
Методические указания: основное внимание должно быть уделено освоению аддитивной группы эллиптической кривой.

Раздел 3. Протоколы на эллиптических кривых
Тема 8. Криптосистемы на эллиптических кривых.
Цель работы: ознакомиться с протоколами на эллиптических кривых.
Задание. Написать программу, с помощью которой реализуема адаптация протокола Диффи-Хеллмана для эллиптических кривых.
Методические указания: основное внимание должно быть уделено освоению методов построений протоколов на эллиптических кривых.
Тема 8. Криптосистемы на эллиптических кривых.
Цель работы: ознакомиться с протоколами на эллиптических кривых.
Задание. Написать программу, реализующую электронную подпись ГОСТ Р 34.10-2012.
Методические указания: основное внимание должно быть уделено освоению методов построений протоколов на эллиптических кривых.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Перечень направлений исследования для курсовых работ

1. Построение конечных полей.
2. Криптосистемы Эль-Гамаля на эллиптических кривых.
3. Криптосистема Месси-Омуры на эллиптической кривой.
4. Рюкзачная криптосистема Шора-Ривеста на основе конечных полей.

5. Совершенные шифры на основе ортогональных таблиц.
6. Российский стандарт электронной подписи ГОСТ Р 34.10-2012
7. Американские стандарты электронной подписи RDS и ECDSA.
8. Реализация протокола аутентификации Шнорра на эллиптических кривых.
9. Реализация протокола аутентификации Окамото на эллиптических кривых.
10. Дискретное логарифмирование на эллиптической кривой.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ (ЭКЗАМЕНУ)

1. Китайская теорема об остатках для идеалов колец. Разложение кольца вычетов в прямую сумму примарных колец.
2. Поле: определение и основные свойства. Подполе. Критерий подполя. Критерий конечного подполя.
3. Простые поля. Характеристика поля.
4. Расширение поля. Теорема о башне полей.
5. Алгебраические и трансцендентные элементы поля. Простые расширения полей. Теорема о классификации простых расширений полей.
6. Поле разложения многочлена.
7. Конечные поля. Построение конечного поля.
8. Образующие элементы конечного поля.
9. Неприводимые многочлены над конечными полями.
10. Блочный шифр «Кузнечик» из ГОСТ Р 34.12-2015.
11. Рюкзачная криптосистема Шора-Ривеста на основе конечных полей.
12. Аффинные алгебраические многообразия. Примеры алгебраических многообразий и их идеалов.
13. Проективная плоскость.
14. Эллиптические кривые: определение, общая форма Вейерштрасса эллиптической кривой.
15. Сложение точек эллиптической кривой над полем **R**.
16. Сложение точек эллиптической кривой над конечным полем.
17. Модификация системы Диффи-Хеллмана на эллиптических кривых.
18. Вероятностное шифрование на основе эллиптических кривых, модификация шифра Эль-Гаамаля.
19. Модификация протокола Месси-Омуры на эллиптических кривых.
20. Модификация схемы разделения секрета Фельдмана-Шамира на эллиптических кривых.
21. Модификация схемы разделения секрета Педерсона-Шамира на эллиптических кривых.
22. Модификация протокола аутентификации Шнорра на эллиптических кривых.
23. Модификация трехпроходного протокола аутентификации Шнорра на эллиптических кривых.
24. Модификация протокола аутентифкации Окамото на эллиптических кривых.
25. Модификация протокола аутентификации с нулевым разглашением на основе системы Диффи-Хеллмана с использованием эллиптических кривых.
26. Модификация протокола аутентификации с нулевым разглашением на основе шифра Эль-Гамаля с использованием эллиптических кривых.
27. Модификация семейства протоколов MTI на эллиптических кривых.
28. Протокол привязки к биту на основе протокола Шнорра с использованием эллиптических кривых.
29. Протокол типа “подбрасывание монеты по телефону” с использованием эллиптических кривых.

30. Электронная подпись ГОСТ Р 34.10-2012.
31. Электронная подпись ECDSA.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Группы. Кольца.	Проработка учебного материала, подготовка к сдаче зачета и экзамена	8	Зачет, экзамен
2. Поля.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета и экзамена	18	Зачет, экзамен, проверка лабораторных работ
3. Применение конечных полей в криптографии.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета и экзамена, решение задач	20	Зачет, экзамен, проверка лабораторных работ, проверка решения задач
4. Аффинные алгебраические многообразия.	Проработка учебного материала, подготовка к сдаче зачета и экзамена	6	Зачет, экзамен
5. Проективная плоскость.	Проработка учебного материала, подготовка к сдаче зачета и экзамена	6	Зачет, экзамен
6. Эллиптические кривые.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета и экзамена, решение задач	10	Зачет, экзамен, проверка лабораторных работ, проверка решения задач
7. Выбор точки и размещение данных.	Проработка учебного материала, подготовка к сдаче зачета и экзамена	2	Зачет, экзамен
8. Криптосистемы на эллиптических кривых.	Проработка учебного материала, лабораторные работы, подготовка к сдаче зачета и экзамена, решение задач	18	Зачет, экзамен, проверка лабораторных работ, проверка решения задач
9.Дискретное логарифмирование на эллиптической кривой	Проработка учебного материала, подготовка к сдаче зачета и экзамена	8	Зачет, экзамен

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Васильева И.Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. Москва : Издательство Юрайт, 2019. 349 с. (Серия : Бакалавр. Академический курс). ISBN 978-5-534-02883-6. Текст : электронный // ЭБС Юрайт [сайт]. URL: https://biblio-online.ru/bcode/433610
2. Рацеев С.М. Математические методы защиты информации : электронный учебный курс / С. М. Рацеев; УлГУ, ФМИАТ. - Ульяновск : УлГУ, 2018. — URL: http://edu.ulsu.ru/cources/921/interface

дополнительная

1. Поднебесова Г.Б. Абстрактная и компьютерная алгебра [Электронный ресурс]: практикум/ Поднебесова Г.Б.— Электрон. текстовые данные.— Челябинск: Южно-Уральский государственный гуманитарно-педагогический университет, 2016.— 125 с.— Режим доступа: http://www.iprbookshop.ru/83852.html
2. ГОСТ-Эксперт – единая база ГОСТов Российской Федерации для образования и промышленности:
   2.1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: https://gostexpert.ru/gost/gost-34.10-2012
   2.2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования. М.: Стандартинформ, 2013. — URL: https://gostexpert.ru/gost/gost-34.11-2012

учебно-методическая

1. Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск : УлГУ, 2016. 55 с. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/270
2. Рацеев С.М. Лабораторный практикум по методам алгебраической геометрии в криптографии / С. М. Рацеев; УлГУ, ФМИАТ, Каф. информ. безопасности и теории управления. - Ульяновск : УлГУ, 2019. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/1344
3. 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; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 159 КБ). - Текст : электронный. Режим доступа: http://lib.ulsu.ru/MegaPro/Download/MObject/4680

Согласовано:

Гл.библ-рь НБ УлГУ	Полина И.Ю		04.05.2021
должность сотрудника научной библиотеки	ФИО	подпись	дата

б) Программное обеспечение

Для образовательного процесса по данной дисциплине необходим стационарный класс ПК с установленным следующим программным обеспечением:

- операционная среда ОС Windows/Linux;
- системы программирования на языках Си/С++ (Code::Blocks).

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. IPRbooks : электронно-библиотечная система : сайт / группа компаний Ай Пи Ар Медиа. - Саратов, [2021]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. ЮРАЙТ : электронно-библиотечная система : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2021]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. Консультант студента : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2021]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача : электронно-библиотечная система : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2021]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2021]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2021]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. **Znanium.com :** электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2021]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

1.8. Clinical Collection : коллекция для медицинских университетов, клиник, медицинских библиотек // EBSCOhost : [портал]. – URL: http://web.b.ebscohost.com/ehost/search/advanced?vid=1&sid=9f57a3e1-1191-414b-8763-e97828f9f7e1%40sessionmgr102 . – Режим доступа : для авториз. пользователей. – Текст : электронный.

1.9. Русский язык как иностранный : электронно-образовательный ресурс для иностранных студентов : сайт / ООО Компания «Ай Пи Ар Медиа». – Саратов, [2021]. – URL: https://ros-edu.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2021].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий : электронные журналы / ООО ИВИС. - Москва, [2021]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2021]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. «Grebennikon» : электронная библиотека / ИД Гребенников. – Москва, [2021]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Национальная электронная библиотека : электронная библиотека : федеральная государственная информационная система : сайт / Министерство культуры РФ ; РГБ. – Москва, [2021]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase // EBSCOhost : [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://window.edu.ru/ . – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАОУ ДПО ЦРГОП и ИТ. – URL: http://www.edu.ru. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

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

Согласовано:

Зам.нач. УИТиТ	/ Клочкова А.В.	/	04.05.2021
должность сотрудника УИТиТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аудитория -3/316. Аудитория для проведения лекционных, семинарских и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. Комплект переносного мультимедийного оборудования: ноутбук с выходом в Интернет, экран, проектор, Wi-Fi с доступом в Интернет, ЭИОС,ЭБС. 432017, Ульяновская область, г. Ульяновск, ул. Набережная реки Свияги, д. 106-3 корпус

Аудитория 24б для проведения лабораторных и практических занятий, текущего контроля и промежуточной аттестации, групповых и индивидуальных консультаций. 11 персональных компьютеров, проектор, экран, системы защиты информации: Соболь, Аккорд, Dallas Lock, Secret Net Studio. Сервер Vimark, АПКШ "Континент", Маршрутизаторы Cisco, Система защиты информации ViPNet. 432017, Ульяновская обл, г Ульяновск, ул Набережная реки Свияги, д 106-2 корпус

Аудитория -230. Аудитория для самостоятельной работы. Аудитория укомплектована ученической мебелью. 16 персональных компьютеров. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус

Аудитория -237. Читальный зал научной библиотеки с зоной для самостоятельной работы. Аудитория укомплектована ученической мебелью. Компьютерная техника, телевизор, экран, проектор. Стол для лиц с ОВЗ. 432017, Ульяновская область, г. Ульяновск, р-н Железнодорожный, ул. Набережная р. Свияги, № 106-1 корпус.

Реализация программы дисциплины требует наличия учебной лаборатории. Оборудование учебной лаборатории: посадочные места по количеству студентов. Технические средства обучения: компьютеры с лицензионным программным обеспечением:

- операционная среда ОС Windows/ Альт Рабочая станция 8;
- системы программирования на языках Си/С++ (Code::Blocks, Visual Studio).

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

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

- для лиц с нарушением зрения: в форме электронного документа, индивидуальные консультации с привлечением тифлосурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением слуха: в форме электронного документа, индивидуальные консультации с привлечением сурдопереводчика, индивидуальные задания и консультация;
- для лиц с нарушением опорно-двигательного аппарата: в форме электронного документа, индивидуальные задания и консультация.

Разработчик _____ / Ганеев С.М. /
подпись ФИО