УТВЕРЖДЕНО
решением Ученого совета факультета математики, информационных и авиационных технологий
от «21» мая 2024 г., протокол № 5/24

Председатель _____ / М.А. Волков
«21» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Криптографические методы защиты информации**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	4 - очная форма обучения

Направление (специальность): 02.03.03 Математическое обеспечение и администрирование информационных систем
Направленность (профиль/специализация): Технология программирования
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 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	Кафедра информационной безопасности и теории управления	Профессор,Доктор физико-математических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

- приобретение общих представлений о криптографических методах и средствах обеспечения информационной безопасности;
- знакомство с важнейшими криптоалгоритмами, принципами их построения.

Задачи освоения дисциплины:

- освоение основных методов выбора алгоритмов для различных применений и оценки их качества;
- дать основы системного подхода к организации защиты информации; принципов синтеза и анализа шифров;
- дать основы математических методов, используемых в криптоанализе.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Криптографические методы защиты информации» относится к числу дисциплин блока Б1.В.1, предназначенного для студентов, обучающихся по направлению: 02.03.03 Математическое обеспечение и администрирование информационных систем.

В процессе изучения дисциплины формируются компетенции: ПК-2, ПК-3, ПК-4, ПК-5.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Эксплуатационная практика, Проектно-технологическая практика, Проектная деятельность, Подготовка к сдаче и сдача государственного экзамена, Проектирование информационных систем, Современные системы автоматизации разработки информационных систем, Разработка мобильных приложений, Инструментальные средства для визуального программирования, Программирование для Интернет, Высокопроизводительные вычисления, Программирование на языке Java, Информационные сети, 1С: Предприятие для программистов и системных администраторов, Открытые технологии разработки программного обеспечения, Обнаружение вторжений и защита информации, Объектно-ориентированное программирование, Системы реального времени, Метрология, стандартизация и сертификация информационных технологий, Компьютерная геометрия и графика, Методы программирования современных информационных систем, Администрирование информационных систем, Преддипломная практика, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Методы разработки программного обеспечения, Технологическая (проектно-технологическая) практика, Представление знаний, Параллельное программирование, Методы и системы обработки больших данных, Сетевое программирование, Функциональное программирование, Интеллектуальные системы и технологии, Методы машинного обучения, Операционные системы, Графический дизайн, Базы данных, Web-технологии, Системы принятия решений, Имитационное моделирование, Теория систем и системный анализ, Численные методы, Управление стартапами в технологическом предпринимательстве.

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**
ПК-2 Способен использовать основные методы и средства автоматизации проектирования, реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта и программных комплексов, а также способен использовать методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов	**знать**: основные задачи, решаемые криптографическими методами **уметь**: проводить вычисления в числовых и конечных кольцах и полях с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ **владеть**: криптографической терминологией
ПК-3 Способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств; операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности	**знать**: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров. **уметь**: корректно применять симметричные и асимметричные криптографические алгоритмы **владеть**: криптографической терминологией
ПК-4 Способен использовать основные концептуальные положения функционального, логического, объектно-ориентированного и визуального направлений программирования, методы, способы и средства разработки программ в рамках этих направлений	**знать**: зарубежные и российские криптографические стандарты **уметь**: корректно применять симметричные и асимметричные криптографические алгоритмы **владеть**: криптографической терминологией
ПК-5 Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	**знать**: основные виды симметричных и асимметричных криптографических алгоритмов; математические модели шифров. **уметь**: корректно применять симметричные и асимметричные криптографические алгоритмы **владеть**: криптографической терминологией

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 3 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 108 часов

Форма обучения: очная

Вид учебной работы	**Количество часов (форма обучения очная)**	
	Всего по плану	**В т.ч. по семестрам**
		7
1	**2**	**3**
Контактная работа обучающихся с преподавателем в соответствии с УП	54	54
Аудиторные занятия:	54	54
Лекции	18	18
Семинары и практические занятия	18	18
Лабораторные работы, практикумы	18	18
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование, Оценивание выполнения задания	Тестирование, Оценивание выполнения задания
Курсовая работа	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачёт	Зачёт
Всего часов по дисциплине	108	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. Надежность шифров							
Тема 1.1. Шифры замены и перестановки	16	2	2	4	0	8	Тестирование, Оценивание выполнения задания
Тема 1.2. С	20	4	4	0	0	12	Тестирова

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
овершенные шифры							ние
Раздел 2. Схемы разделения секрета							
Тема 2.1. Пороговые схемы разделения секрета	16	2	2	4	0	8	Тестирование, Оценивание выполнения задания
Тема 2.2. Схемы разделения секрета с произвольной структурой доступа	8	2	2	0	0	4	Тестирование, Оценивание выполнения задания
Раздел 3. Блочные шифры и электронные подписи							
Тема 3.1. Симметричные блочные шифры	28	4	4	6	0	14	Тестирование
Тема 3.2. Шифрование с открытым ключом	20	4	4	4	0	8	Тестирование, Оценивание выполнения задания
Итого подлежит изучению	108	18	18	18	0	54	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Надежность шифров

Тема 1.1. Шифры замены и перестановки

Шифр простой замены. Шифр сдвига. Методы взлома данного шифра. Аффинный шифр и методы его взлома. Преобразование биграмм аффинным шифром. Шифр замены с конечным ключом. Шифр Виженера. Криптоанализ шифра Виженера. Многопетлевые подстановки.

Аффинный блочный шифр. Шифр Холла. Криптоанализ аффинного блочного шифра. Табличное гаммирование. Модульное гаммирование. Шифр Вернама. Шифр пропорциональной замены (шифр омофонов). Маршрутные перестановки. Криптоанализ шифров. Детерминированная модель открытого текста. Вероятностная модель независимых символов алфавита. Вероятностная модель независимых биграмм. Вероятностная модель марковски зависимых символов. Критерии распознавания открытых текстов. Критерий на основе проверки гипотезы с использованием леммы Неймана-Пирсона. Критерий на основе запретных m-грамм.

Тема 1.2. Совершенные шифры

Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей. Пример совершенного неэндоморфного шифра с равномерным распределением на множестве ключей. Пример совершенного эндоморфного шифра с неравномерным распределением на множестве ключей. Пример совершенного неэндоморфного шифра с неравномерным распределением на множестве ключей. Примеры совершенных шифров. (k|y)-совершенные шифры: определение, эквивалентные условия. Необходимые и достаточные условия (k|y)-совершенных шифров. Необходимые и достаточные условия одновременно совершенных и (k|y)-совершенных шифров. Примеры (k|y)-совершенных шифров. Математические модели шифра замены с ограниченным и неограниченным ключом. Шифрвеличины и шифробозначения. Опорный шифр шифра замены. Степень опорного шифра. Случайный и детерминированный генераторы ключевого потока. Шифр замены с неограниченным ключом. Шифр замены с ограниченным ключом. Совершенные шифры замены. Определение совершенного шифра замены, эквивалентные условия. Несовершенность в общем случае шифра замены с ограниченным ключом. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом в классе эндоморфных шифров. Критерий совершенности шифра замены с неограниченным ключом в классе шифров с равномерным распределением на множестве ключей.

Раздел 2. Схемы разделения секрета

Тема 2.1. Пороговые схемы разделения секрета

Понятие (n,t) пороговой схемы разделения секрета. Пример (n,n) пороговой схемы. Схема разделения секрета на основе решения СЛАУ. Схема разделения секрета Шамира. Проверяемая схема разделения секрета Фельдмана-Шамира. Совершенная проверяемая схема разделения секрета Педерсона-Шамира. Схемы разделения секрета на основе n-разрядных равновесных двоичных кодов.

Тема 2.2. Схемы разделения секрета с произвольной структурой доступа

Структуры доступа, связанные с разбиением множества участников. Схема Ито-Саито-Нишизеки. Схемы для конъюнктивных иерархических структур доступа. Схемы для дизъюнктивных иерархических структур доступа.

Раздел 3. Блочные шифры и электронные подписи

Тема 3.1. Симметричные блочные шифры

Итеративные блочные шифры. Понятие раундовой функции, раундового ключа. Условия, обеспечивающие обратимость итеративного блочного шифра. Построение цикловой функции. Входное и выходное отображения. Слабые ключи итеративного блочного шифра. Определение шифра Фейстеля. Функция усложнения шифра Фейстеля. Условия, обеспечивающие обратимость шифра Фейстеля. Примеры итеративных блочных шифров. Шифры “Магма” и “Кузнечик” из ГОСТ Р 34.12-2015. Шифр AES. Режим электронной кодовой книги. Режим сцепления блоков. Режим гаммирования с обратной связью по шифртексту. Режим гаммирования. Режим выработки имитовставки. Свойства данных режимов.

Тема 3.2. Шифрование с открытым ключом

Задачи, приводящие к криптографии с открытым ключом. Понятие односторонней функции. Быстрое (бинарное) возведение в степень. Система Диффи-Хеллмана. Способы выбора образующего элемента. Модификация системы Диффи-Хеллмана на эллиптических кривых. Криптосистема без передачи ключа (шифр Шамира). Описание системы. Надежность системы. Модификация системы на эллиптических кривых. Шифр Эль-Гамаля. Ограничения на параметры системы. Модификация шифра Эль-Гамаля на эллиптических кривых. Шифр RSA. Понятие односторонней функции с «лазейкой». Описание шифра RSA. Ограничения на параметры системы. Рюкзачные системы. Описание «проблемы рюкзака». Система Меркла-Хеллмана на основе супервозрастающей последовательности. Криптосистема Шора-Ривеста на основе конечных полей.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Надежность шифров

Тема 1.1. Шифры замены и перестановки

Вопросы к теме:

Очная форма

Шифр простой замены. Шифр сдвига. Методы взлома данного шифра. Аффинный шифр и методы его взлома. Преобразование биграмм аффинным шифром. Шифр замены с конечным ключом. Шифр Виженера. Криптоанализ шифра Виженера. Многопетлевые подстановки. Аффинный блочный шифр. Шифр Холла. Криптоанализ аффинного блочного шифра. Табличное гаммирование. Модульное гаммирование. Шифр Вернама. Шифр пропорциональной замены (шифр омофонов). Маршрутные перестановки. Криптоанализ шифров.

Тема 1.2. Совершенные шифры

Вопросы к теме:

Очная форма

Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра. Достаточное условие совершенного по Шеннону шифра. Теорема Шеннона. Критерий совершенных шифров в классе шифров с равномерным распределением вероятностей на множестве ключей. Пример совершенного неэндоморфного шифра с равномерным распределением на множестве ключей. Пример совершенного эндоморфного шифра с неравномерным распределением на множестве ключей. Пример совершенного неэндоморфного шифра с неравномерным распределением на множестве ключей. (k|y)-совершенные шифры: определение, эквивалентные условия. Необходимые и достаточные условия (k|y)-совершенных шифров. Необходимые и достаточные условия одновременно совершенных и (k|y)-совершенных шифров. Математические модели шифра замены с ограниченным и неограниченным ключом. Шифрвеличины и шифробозначения. Опорный шифр шифра замены. Степень опорного шифра. Случайный и детерминированный генераторы ключевого потока. Шифр замены с неограниченным ключом. Шифр замены с ограниченным ключом. Совершенные шифры замены. Определение совершенного шифра замены, эквивалентные условия. Несовершенность в общем случае шифра замены с ограниченным ключом. Достаточные условия совершенного шифра замены с неограниченным ключом. Критерий совершенности шифра замены с неограниченным ключом в классе эндоморфных шифров. Критерий совершенности шифра замены с неограниченным ключом в классе шифров с равномерным распределением на множестве ключей.

Раздел 2. Схемы разделения секрета

Тема 2.1. Пороговые схемы разделения секрета

Вопросы к теме:

Очная форма

Понятие (n,t) пороговой схемы разделения секрета. Пример (n,n) пороговой схемы. Схема разделения секрета на основе решения СЛАУ. Схема разделения секрета Шамира. Проверяемая схема разделения секрета Фельдмана-Шамира. Совершенная проверяемая схема разделения секрета Педерсона-Шамира. Схемы разделения секрета на основе n-разрядных равновесных двоичных кодов.

Тема 2.2. Схемы разделения секрета с произвольной структурой доступа

Вопросы к теме:

Очная форма

Схемы разделения секрета для произвольных структур доступа: основные понятия. Схема Бенало-Лейхтера. Схема Ито-Саито-Нишизеки.

Раздел 3. Блочные шифры и электронные подписи

Тема 3.1. Симметричные блочные шифры

Вопросы к теме:

Очная форма

Итеративные блочные шифры. Понятие раундовой функции, раундового ключа. Условия, обеспечивающие обратимость итеративного блочного шифра. Построение цикловой функции. Входное и выходное отображения. Слабые ключи итеративного блочного шифра. Определение шифра Фейстеля. Функция усложнения шифра Фейстеля. Условия, обеспечивающие обратимость шифра Фейстеля. Примеры итеративных блочных шифров. Шифры “Магма” и “Кузнечик” из ГОСТ Р 34.12-2015. Шифр AES.

Тема 3.2. Шифрование с открытым ключом

Вопросы к теме:

Очная форма

Задачи, приводящие к криптографии с открытым ключом. Понятие односторонней функции. Быстрое (бинарное) возведение в степень. Система Диффи-Хеллмана. Способы выбора образующего элемента. Модификация системы Диффи-Хеллмана на эллиптических кривых. Криптосистема без передачи ключа (шифр Шамира). Описание системы. Надежность системы. Модификация системы на эллиптических кривых. Шифр Эль-Гамаля. Ограничения на параметры системы. Модификация шифра Эль-Гамаля на эллиптических кривых. Шифр RSA. Понятие односторонней функции с «лазейкой». Описание шифра RSA. Ограничения на параметры системы. Рюкзачные системы. Описание «проблемы рюкзака». Система Меркла-Хеллмана на основе супервозрастающей последовательности. Криптосистема Шора-Ривеста на основе конечных полей.

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Шифры замены и перестановки
Цели: Исследование шифров замены и перестановки
Содержание: Разработать криптографическую защиту информации, содержащейся в текстовом (двоичном) файле данных, с помощью алгоритма шифрования, указанного в варианте.
Результаты: основное внимание должно быть уделено освоению классических шифров
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Пороговые схемы разделения секрета
Цели: изучение -пороговых схем разделения секрета
Содержание: Реализовать схему разделения секрета в соответствии с индивидуальным вариантом. Программа должна уметь как разделять секрет на участников в соответствии с порогом , так и восстанавливать его. Варианты заданий: 1. Схема разделения секрета Шамира. 2. Схема разделения секрета на основе равновесных двоичных кодов. 3. Схема разделения секрета на основе китайской теоремы об остатках.
Результаты: основное внимание должно быть уделено освоению принципов построения схем разделения секрета

Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Симметричные блочные шифры
Цели: ознакомиться с шифрованием и расшифрованием информации при помощи алгоритма “Магма” из ГОСТ Р 34.12-2015.
Содержание: Реализовать шифр “Магма” из ГОСТ Р 34.12-2015 и основные режимы шифрования.
Результаты: основное внимание должно быть уделено освоению шифра “Магма” из ГОСТ Р 34.12-2015 и основных режимов шифрования.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Шифрование с открытым ключом
Цели: освоить обмен ключами по схеме Диффи-Хеллмана, изучая проблему первообразных корней.
Содержание: Реализовать программу, генерирующую алгоритм обмена ключей по схеме Диффи-Хеллмана.
Результаты: основное внимание должно быть уделено освоению ассиметричных шифров.
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 ЗАЧЕТУ

1. Одноалфавитные шифры замены: аффинный шифр, преобразование биграмм аффинным шифром. Методы взлома данных шифров.

2. Многоалфавитные шифры замены. Шифр Виженера. Криптоанализ шифра Виженера.

3. Многоалфавитные шифры замены: многопетлевые подстановки, аффинный блочный шифр, шифр Холла. Криптоанализ аффинного блочного шифра.

4. Одноалфавитные шифры замены: шифр простой замены, шифр сдвига. Методы взлома данных шифров.

5. Алгебраическая и вероятностная модели шифров.

6. Математическая модель некоторых шифров: шифр простой замены, шифр сдвига, аффинный шифр.

7. Математическая модель некоторых шифров: шифр замены с конечным ключом, шифр Виженера, шифр перестановки.

8. Определение совершенного по Шеннону шифра. Эквивалентные условия. Необходимые условия совершенного по Шеннону шифра.

9. Понятие (n,t) пороговой схемы разделения секрета. Пример (n,n) пороговой схемы. Схема

разделения секрета на основе решения СЛАУ.

10. Схема разделения секрета Шамира.

11. Проверяемая схема разделения секрета Фельдмана-Шамира.

12. Совершенная проверяемая схема разделения секрета Педерсона-Шамира.

13. Схемы разделения секрета для произвольных структур доступа: основные понятия. Схема Бенало-Лейхтера.

14. Схема Ито-Саито-Нишизеки.

15. Итеративные блочные шифры. Обратимость итеративного блочного шифра.

16. Режимы использования симметричных блочных шифров.

17. Шифр Магма из ГОСТ Р 34.12-2015.

18. Схема Диффи-Хеллмана.

19. Вероятностный шифр Эль-Гамаля.

20. Шифр RSA.

21. Рюкзачные криптосистемы.

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. Надежность шифров			
Тема 1.1. Шифры замены и перестановки	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование, Оценивание выполнения задания
Тема 1.2. Совершенные шифры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	12	Тестирование
Раздел 2. Схемы разделения секрета			
Тема 2.1. Пороговые схемы разделения секрета	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование, Оценивание выполнения задания
Тема 2.2. Схемы разделения секрета с произвольной структурой доступа	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование, Оценивание выполнения задания
Раздел 3. Блочные шифры и электронные подписи			
Тема 3.1. Симметричные блочные шифры	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	14	Тестирование
Тема 3.2. Шифрование с открытым ключом	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	8	Тестирование, Оценивание выполнения задания

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы
основная

1. Васильева Ирина Николаевна. Криптографические методы защиты информации : Учебник и практикум Для академического бакалавриата / И.Н. Васильева ; Васильева И. Н. - Москва : Юрайт,

2017. - 349 с. - (Высшее образование). - URL: https://urait.ru/bcode/402115 (дата обращения: 26.10.2021). - Режим доступа: Электронно-библиотечная система Юрайт, для авториз. пользователей. - Электрон. дан. - ISBN 978-5-534-02883-6 : 829.00. / .— ISBN 0_277991

2. 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

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. Фомичев, В. М. Сборник задач по криптологии : сборник задач для студентов, обучающихся по направлению: 10.03.01 «информационная безопасность», профиль: «комплексная защита объектов информации» / В. М. Фомичев ; В. М. Фомичев. - Москва : Прометей, 2019. - 104 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - Текст. - Весь срок охраны авторского права. - электронный. - Электрон. дан. (1 файл). - URL: http://www.iprbookshop.ru/94524.html. - Режим доступа: ЭБС IPR BOOKS; для авторизир. пользователей. - ISBN 978-5-907100-39-8. / .— ISBN 0_153978

учебно-методическая

1. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Криптографические методы защиты информации» для студентов направлений подготовки 02.03.03 «Математическое обеспечение и администриро- вание информационных систем» и 09.03.03 «Прикладная информатика» / С. М. Рацеев. - 2022. - 10 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13408. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_476031.

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