МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА"

СОГЛАСОВАНО
Зав. выпускающей кафедры

УТВЕРЖДАЮ

Защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Вычислительной и прикладной математики**

Учебный план 09.03.04_24_00_ МГТУ.plx
09.03.04 Программная инженерия

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	16	16	16	16
Практические	16	16	16	16
Иная контактная работа	0,25	0,25	0,25	0,25
Итого ауд.	64,25	64,25	64,25	64,25
Контактная работа	64,25	64,25	64,25	64,25
Сам. работа	35	35	35	35
Часы на контроль	8,75	8,75	8,75	8,75
Итого	108	108	108	108

г. Рязань

Программу составил(и):
к.т.н., доц., Тишкина Валерия Валентиновна

Рабочая программа дисциплины
Защита информации

разработана в соответствии с ФГОС ВО:
ФГОС ВО - бакалавриат по направлению подготовки 09.03.04 Программная инженерия (приказ Минобрнауки России от 19.09.2017 г. № 920)

составлена на основании учебного плана:
09.03.04 Программная инженерия
утвержденного учёным советом вуза от 26.01.2024 протокол № 8.

Рабочая программа одобрена на заседании кафедры
Вычислительной и прикладной математики

Протокол от 19.06.2024 г. № 10
Срок действия программы: 20242028 уч.г.
Зав. кафедрой Овечкин Геннадий Владимирович

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Вычислительной и прикладной математики

Протокол от __ _____ 2025 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Вычислительной и прикладной математики

Протокол от __ _____ 2026 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Вычислительной и прикладной математики

Протокол от __ _____ 2027 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры

Вычислительной и прикладной математики

Протокол от __ _____ 2028 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цели:
1.2	1. Получение знаний о методах защиты информации, ее сохранности и конфиденциальности, а также о методах обеспечения информационной безопасности.
1.3	2. Освоение навыков работы с различными средствами защиты информации и их применение в процессе разработки программного обеспечения.
1.4	3. Развитие навыков анализа существующих угроз информационной безопасности и способов их предотвращения.
1.5	4. Приобретение практического опыта работы с защитой информации на практике.
1.6	
1.7	Задачи:
1.8	1. Изучение основных принципов защиты информации.
1.9	2. Освоение современных методов криптографической защиты данных и других методов защиты информации.
1.10	3. Получение навыков работы с средствами защиты информации, такими как антивирусы, файрволы, IDS/IPS системы и другие.
1.11	4. Изучение основных угроз информационной безопасности и методов защиты от них.
1.12	5. Проведение практических работ по обеспечению безопасности IT-систем.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Архитектура ЭВМ
2.1.2	Программирование
2.1.3	Теория вероятностей
2.1.4	Логика и теория алгоритмов
2.1.5	Операционные системы
2.1.6	Выполнение и защита ВКР
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Подготовка и защита ВКР
2.2.2	Тестирование ПО
2.2.3	Экономика программной инженерии

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-1: Владеет навыками использования различных технологий разработки программного обеспечения, включая современные

ПК-1.1. Руководит процессом разработки программного обеспечения

Знать
методы проектирования программного обеспечения и его программную реализации.
Уметь
применять методы проектирования программного обеспечения и его программную реализацию.
Владеть
навыками проектирования программного обеспечения и его программной реализацией.

ПК-1.2. Руководит проверкой работоспособности программного обеспечения

Знать
базовые способы проверки работоспособности программного обеспечения, а также наиболее простые способы интеграции программных модулей и компонентов.
Уметь
проводить проверку работоспособности и рефакторинг кода программного обеспечения.
Владеть
методами проверки работоспособности кода программного обеспечения, интеграции программных модулей и компонентов разнообразных информационных систем, для большинства платформ и операционных систем.

ПК-1.3. Организует внедрение и сопровождение разработанного программного обеспечения

Знать
методологию внедрения программного обеспечения.
Уметь
осуществлять разработку, документирование всех настроек, создавать систему поддержки и адекватное обучение пользователей.
Владеть
всеми этапами сопутствующими внедрению и сопровождению разработанного программного обеспечения.

ПК-2: Способен классифицировать и идентифицировать задачи искусственного интеллекта, выбирать адекватные методы и инструментальные средства решения задач искусственного интеллекта

ПК-2.1. Классифицирует и идентифицирует задачи систем искусственного интеллекта в зависимости от особенностей проблемной и предметной областей

Знать
классы решаемых задач с помощью систем искусственного интеллекта, основные параметры идентификации задач искусственного интеллекта: назначение, сфера применения, виды используемых знаний, временные аспекты решения задач.
Уметь
определять принадлежность проблемной области к классу решаемых задач с помощью систем искусственного интеллекта и основные параметры идентификации задач систем искусственного интеллекта.
Владеть
особенностями классификации и идентификации задач искусственного интеллекта для различных предметных областей.

ПК-3: Способен разрабатывать и тестировать программные компоненты решения задач в системах искусственного интеллекта

ПК-3.3. Проводит тестирование систем искусственного интеллекта

Знать
основные критерии качества систем искусственного интеллекта, методы и инструментальные средства тестирования работоспособности и качества функционирования систем искусственного интеллекта.
Уметь
проводить тестирование работоспособности и качества функционирования систем искусственного интеллекта и проверять выполнение требований к системам искусственного интеллекта со стороны пользователя.
Владеть
методологией тестирования систем искусственного интеллекта. Методами настройки программного обеспечения и компонентов систем искусственного интеллекта.

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	Теоретические основы защиты информации;
3.1.2	Алгоритмы защиты информации и их практическая реализация;
3.1.3	Защита программ от нелегального копирования;
3.1.4	Методы и алгоритмы сжатия данных.
3.1.5	
3.1.6	
3.2	**Уметь:**
3.2.1	Применять методы проектирования программного обеспечения и его программную реализацию;
3.2.2	Осуществлять сбор и обобщение информации о проблемной области путем опроса экспертов, исходных данных о функционировании проблемной области
3.2.3	
3.2.4	
3.3	**Владеть:**
3.3.1	Реализации электронного аналога шифровальной машины «Энигма»;
3.3.2	Реализации алгоритма шифрования с открытым ключом (RSA);
3.3.3	Реализации алгоритма симметричного шифрования (AES);
3.3.4	Реализации алгоритма симметричного шифрования (DES)

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Форма контроля
	Раздел 1. Защита информации					
1.1	Теоретические основы защиты информации. /Тема/	7	0			

1.2	Введение в предметную область, изложение основных понятий, определения, освещение исторического контекста защиты информации. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.3	Защита программ от нелегального копирования. Проектирование информационных систем с точки зрения безопасности. Моделирование угроз и нарушителей. Риски.Требования к алгоритмам шифрования. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.4	Правило Огюста Керкхоффа. Симметричные алгоритмы. Поточное шифрование. Блочные алгоритмы. Шифры перестановки. Шифры замены. Моно- и полиалфавитные шифры. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.5	Индекс соответствия. Шифровальная машина Энигма. Шифрование с открытым ключом. Применение генераторов случайных чисел. Алгоритм Фон Неймана. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.6	Реализация электронного аналога шифровальной машины «Энигма» /Лаб/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

1.7	Реализация алгоритма шифрования с открытым ключом (RSA) /Лаб/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.8	Реализация электронного аналога шифровальной машины «Энигма» /Пр/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.9	Реализация алгоритма шифрования с открытым ключом (RSA) /Пр/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.10	Введение в предметную область, изложение основных понятий, определения, освещение исторического контекста защиты информации. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.11	Защита программ от нелегального копирования. Проектирование информационных систем с точки зрения безопасности. Моделирование угроз и нарушителей. Риски.Требования к алгоритмам шифрования. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

1.12	Правило Огюста Керкхоффа. Симметричные алгоритмы. Поточное шифрование. Блочные алгоритмы. Шифры перестановки. Шифры замены. Моно- и полиалфавитные шифры. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.13	Индекс соответствия. Шифровальная машина Энигма. Шифрование с открытым ключом. Применение генераторов случайных чисел. Алгоритм Фон Неймана. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.14	Алгоритмы защиты информации и их практическая реализация. /Тема/	7	0			
1.15	Алгоритм на числах Фибоначи. Линейный конгруэнтный генератор. Квадратичный конгруэнтный генератор. Нормальное (Гауссово) распределение. Особенности практического применения симметричного шифрования. Примеры алгоритмов шифрования. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.16	Алгоритм DataEncryptionStandard (DES). Этапы шифрования DES. Функция Фейстеля. Взлом шифра DES. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.17	Открытый конкурс NationalInstituteofStandardsandTechnology (NIST). Алгоритм AdvancedEncryptionStandard. История и особенности асимметричного шифрования. Алгоритм RSA. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

1.18	Алгоритмы определения простоты числа. Решето Эратосфена. Тест Миллера-Рабина. Алгоритм Евклида. Расширенный алгоритм Евклида. Алгоритм быстрого возведения в степень. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.19	Реализация алгоритма шифрования с открытым ключом (RSA) /Лаб/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.20	Реализация алгоритма симметричного шифрования (DES) /Лаб/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.21	Реализация алгоритма симметричного шифрования (AES) /Лаб/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.22	Реализация алгоритма шифрования с открытым ключом (RSA) /Пр/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

1.23	Реализация алгоритма симметричного шифрования (DES) /Пр/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.24	Реализация алгоритма симметричного шифрования (AES) /Пр/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.25	Алгоритм на числах Фибоначи. Линейный конгруэнтный генератор. Квадратичный конгруэнтный генератор. Нормальное (Гауссово) распределение. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.26	Особенности практического применения симметричного шифрования. Примеры алгоритмов шифрования. Алгоритм DataEncryptionStandard (DES). Этапы шифрования DES. Функция Фейстеля. Взлом шифра DES. Усовершенствования DES. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.27	Открытый конкурс NationalInstituteofStandardsandTechnology (NIST). Алгоритм AdvancedEncryptionStandard. История и особенности асимметричного шифрования. Алгоритм RSA. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

1.28	Алгоритмы определения простоты числа. Решето Эратосфена. Тест Миллера-Рабина. Алгоритм Евклида. Расширенный алгоритм Евклида. Алгоритм быстрого возведения в степень. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.29	Вопросы, смежные с криптографией. /Тема/	7	0			
1.30	Методы и алгоритмы сжатия данных. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.31	Алгоритм сжатия Хафмана. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.32	Алгоритм сжатия LZW. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.33	Математическое сжатие. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

1.34	Криптоатаки и методы криптоанализа. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.35	Стеганография. /Лек/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.36	Правовые основы защиты информации. /Лек/	7	4	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.37	Реализация алгоритма симметричного шифрования (AES) /Лаб/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.38	Создание и проверка электронной подписи для документа /Лаб/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

1.39	Реализация алгоритма симметричного шифрования (AES) /Пр/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.40	Создание и проверка электронной подписи для документа /Пр/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.41	Алгоритм сжатия Хафмана. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.42	Алгоритм сжатия LZW. Математическое сжатие. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.43	Криптоатаки и методы криптоанализа. /Ср/	7	3	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

1.44	Стеганография. Правовые основы защиты информации. /Ср/	7	2	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.45	Промежуточная аттестация /Тема/	7	0			
1.46	Подготовка к зачёту /Зачёт/	7	8,75	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.47	Прием зачета /ИКР/	7	0,25	ПК-1.1-З ПК-1.1-У ПК-1.1-В ПК-1.2-З ПК-1.2-У ПК-1.2-В ПК-1.3-З ПК-1.3-У ПК-1.3-В ПК-2.1-З ПК-2.1-У ПК-2.1-В ПК-3.3-З ПК-3.3-У ПК-3.3-В	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2Л3.1 Л3.2	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Основные материалы приведены в приложении к рабочей программе дисциплины (см. документ "Оценочные материалы по дисциплине "Защита информации")

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.1	Башлы П. Н., Бабаш А. В., Баранова Е. К.	Информационная безопасность и защита информации : учебное пособие	Москва: Евразийский открытый институт, 2012, 311 с.	978-5-374-00301-7, http://www.iprbookshop.ru/10677.html

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.2	Евдокимова Л.М., Корябкин В.В., Пылькин А.Н., Швечкова О.Г.	Электронный документооборот и обеспечение безопасности стандартными средствами WINDOWS : учеб. пособие	М.: КУРС, 2017, 294с.; прил.	978-5-906923-24-0,978-5-16-012741-5, 1
Л1.3	Прохорова О. В.	Информационная безопасность и защита информации : учебник для вузов	Санкт-Петербург: Лань, 2023, 124 с.	978-5-507-46010-6, https://e.lanbook.com/book/293009
Л1.4	Швечкова О.Г., Пылькин А.Н., Марчев Д.В.	Базовые криптографические алгоритмы защиты информации: учеб. пособие : Учебное пособие	Рязань: КУРС, 2023,	, https://elib.rsreu.ru/ebs/download/3643

6.1.2. Дополнительная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Нерсесянц А. А.	Защита информации : учебное пособие	Ростов-на-Дону: Северо-Кавказский филиал Московского технического университета связи и информатики, 2010, 61 с.	2227-8397, http://www.iprbookshop.ru/61295.html
Л2.2	Омарова С. А., Искакова К. А., Тойганбаева Н. А.	Информационная безопасность и защита информации : учебно-методический комплекс	Алматы: Нур-Принт, 2012, 98 с.	9965-756-05-8, http://www.iprbookshop.ru/67055.html

6.1.3. Методические разработки

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Каторин Ю. Ф., Разумовский А. В., Спивак А. И., Каторин Ю. Ф.	Техническая защита информации : лабораторный практикум	Санкт-Петербург: Университет ИТМО, 2013, 113 с.	2227-8397, http://www.iprbookshop.ru/68715.html
Л3.2	Малинин Ю.И.	Информационная безопасность и защита информации : Методические указания	Рязань: РИЦ РГРТУ, 2009,	, https://elib.rsreu.ru/ebs/download/851

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Электронная библиотека РГРТУ

6.3 Перечень программного обеспечения и информационных справочных систем

6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование	Описание
PyCharm Community	Свободное ПО
PyCharm	Свободное ПО
Интерпретатор Python	Свободное ПО
Python	Свободно распространяемое программное обеспечение под лицензиями
Python	Свободное ПО

Среда разработки Qt Creator	Свободное ПО
Qt Creator Community	Свободное ПО
Qt	Лицензия Opensource
6.3.2 Перечень информационных справочных систем	
6.3.2.1	Система КонсультантПлюс http://www.consultant.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1	206-1 учебно-административный корпус. Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 42 мест, 1 ПК: ЦП: Intel Pentium 4 class 3200 ОЗУ: 1 Гб ПЗУ: 80 Гб Телевизор: PHILIPS U7PEL4606H/60 документ-камера: AVER Media POB3 (AverVision 330)
2	206-2 учебно-административный корпус. Аудитория для самостоятельной работы 18 мест, Телевизор PHILIPS 46PFL3208T/60; документ-камера: AverVisionF33 POE7D; 20 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Intel Pentium II/III class 2327 ОЗУ: 2 Гб ПЗУ: 80 Гб (1 шт.) ЦП: Intel Pentium III 2992 ОЗУ: 1,5 Гб ПЗУ: 150 Гб (1 шт.) ЦП: Intel Pentium III 2660 ОЗУ: 2 Гб ПЗУ: 80 Гб (9 шт.) ЦП: Intel Pentium III 2793 ОЗУ: 2 Гб ПЗУ: 100 Гб (1 шт.) ЦП: Intel Pentium II/III class 2660 ОЗУ: 1 Гб ПЗУ: 50 Гб (1 шт.) ЦП: Intel Pentium III 2527 ОЗУ: 2 Гб ПЗУ: 100 Гб (1 шт.) ЦП: Intel Pentium III 3158 ОЗУ: 2 Гб ПЗУ: 50 Гб (3 шт.) ЦП: Intel Pentium III 2826 ОЗУ: 2 Гб ПЗУ: 100 Гб (2 шт.) ЦП: Intel Pentium III 2693 ОЗУ: 1,5 Гб ПЗУ: 100 Гб (1 шт.)
3	206-3 учебно-административный корпус. Учебная аудитория для проведения практический занятий, лабораторных работ Проектор: InFocus LP640 18 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Intel Core 2 ОЗУ: 4 Гб ПЗУ: 70 Гб (19 шт.)
4	206-4 учебно-административный корпус. Учебная аудитория для проведения практический занятий, лабораторных работ 18 ПК с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду: ЦП: Pentium 4 class 2800 ОЗУ: 1 Гб ПЗУ: 50 Гб (8 шт.) ЦП: Intel Pentium II/III class 2327 ОЗУ: 2 Гб ПЗУ: 50 Гб (10 шт.)

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)
Методическое обеспечение дисциплины приведено в приложении к рабочей программе дисциплины (см. документ "Методические материалы по дисциплине "Защита информации")