МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра «Вычислительная и прикладная математика»

«СОГЛАСОВАНО»
Заведующий кафедрой ВПМ
_____/ Г.В. Овечкин
_____ 27.01 _____ 2023 г

«УТВЕРЖДАЮ»
Проректор по учебной работе
_____/ А.В. Корячко
_____ 27.01 _____ 2023 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки
09.03.04 Программная инженерия

Направленность (профиль) подготовки
Программное обеспечение систем искусственного интеллекта

Квалификация выпускника — бакалавр

Форма обучения — очная

Рязань 2023 г

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 27.01.2023 протокол № 6.

Рабочая программа одобрена на заседании кафедры
Вычислительной и прикладной математики

Протокол от 29.12.2022 г. № 4
Срок действия программы: 2023-2027 уч.г.
Зав. кафедрой Овечкин Геннадий Владимирович

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

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2024-2025 учебном году на заседании кафедры

Вычислительной и прикладной математики

Протокол от __ _____ 2024 г. № __

Зав. кафедрой _____

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 _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цели:
1.2	Получение знаний о методах защиты информации, ее сохранности и конфиденциальности, а также о методах обеспечения информационной безопасности.
1.3	Освоение навыков работы с различными средствами защиты информации и их применение в процессе разработки программного обеспечения.
1.4	Развитие навыков анализа существующих угроз информационной безопасности и способов их предотвращения.
1.5	Приобретение практического опыта работы с защитой информации на практике.
1.7	Задачи:
1.8	Изучение основных принципов защиты информации.
1.9	Освоение современных методов криптографической защиты данных и других методов защиты информации.
1.10	Получение навыков работы с средствами защиты информации, такими как антивирусы, файрволы, IDS/IPS системы и другие.
1.11	Изучение основных угроз информационной безопасности и методов защиты от них.
1.12	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
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работу

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

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

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.
3.2	**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
3.3	**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-2.1-З ПК-2.1-У ПК-2.1-В 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	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.6	Реализация электронного аналога шифровальной машины «Энигма» /Лаб/	7	3	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.7	Реализация алгоритма шифрования с открытым ключом (RSA) /Лаб/	7	3	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

1.8	Реализация электронного аналога шифровальной машины «Энигма» /Пр/	7	3	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.9	Реализация алгоритма шифрования с открытым ключом (RSA) /Пр/	7	3	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.16	Алгоритм DataEncryptionStandard (DES). Этапы шифрования DES. Функция Фейстеля. Взлом шифра DES. /Лек/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.19	Реализация алгоритма шифрования с открытым ключом (RSA) /Лаб/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.20	Реализация алгоритма симметричного шифрования (DES) /Лаб/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.21	Реализация алгоритма симметричного шифрования (AES) /Лаб/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.22	Реализация алгоритма шифрования с открытым ключом (RSA) /Пр/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

1.23	Реализация алгоритма симметричного шифрования (DES) /Пр/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.24	Реализация алгоритма симметричного шифрования (AES) /Пр/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 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-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.31	Алгоритм сжатия Хафмана. /Лек/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.32	Алгоритм сжатия LZW. /Лек/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.33	Математическое сжатие. /Лек/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

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

1.39	Реализация алгоритма симметричного шифрования (AES) /Пр/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.40	Создание и проверка электронной подписи для документа /Пр/	7	2	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.41	Методы и алгоритмы сжатия данных. /ИКР/	7	0,25	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.42	Алгоритм сжатия Хафмана. /Ср/	7	3	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт
1.43	Алгоритм сжатия LZW. Математическое сжатие. /Ср/	7	3	ПК-2.1-В ПК-2.1-У ПК-2.1-З ПК-1.3-В ПК-1.3-У ПК-1.3-З ПК-1.2-В ПК-1.2-У ПК-1.2-З ПК-1.1-В ПК-1.1-У ПК-1.1-З	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Э1	Зачёт

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

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине представлен в виде оценочных материалов и приведен 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
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

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	Свобродное ПО
Qt Creator Community	Свободное ПО
Qt	Лицензия Opensource

6.3.2 Перечень информационных справочных систем

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.)

8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Методические указания для студентов по освоению дисциплины
Приступая к работе, каждый студент должен принимать во внимание нижеследующие положения.
Дисциплина рассчитана на один семестр (7 семестр).
В седьмом семестре - Зачёт.
На первом занятии студент получает информацию для доступа к комплексу методических материалов по дисциплине.
Лекционные занятия посвящены рассмотрению ключевых, базовых положений курса и разъяснению учебных заданий, выносимых на самостоятельную проработку.
Лабораторные работы и практические занятия предназначены для приобретения опыта практической реализации основной профессиональной образовательной программы. Методические документы к лабораторным работам прорабатываются студентами во время самостоятельной подготовки. Необходимый уровень подготовки контролируется перед сдачей лабораторной работы.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра «Вычислительная и прикладная математика»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ
«Защита информации»

Направление подготовки
09.03.04 «Программная инженерия»

Направленность (профиль) подготовки
«Программное обеспечение систем искусственного интеллекта»

Уровень подготовки – бакалавриат

Квалификация выпускника – бакалавр

Форма обучения – очная

Срок обучения – 4 года

Рязань 2023 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов и процедур, предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной образовательной программы.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций, обучающихся целям и требованиям основной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности компетенций и индикаторов их достижения, приобретаемых обучающимся в соответствии с этими требованиями.

Контроль знаний обучающихся проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости и промежуточная аттестация проводятся с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся, организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся на практических занятиях по результатам выполнения и защиты обучающимися индивидуальных заданий, по результатам выполнения контрольных работ и тестов, по результатам проверки качества конспектов лекций и иных материалов.

В качестве оценочных средств на протяжении семестра используется устные и письменные ответы студентов на индивидуальные вопросы, письменное тестирование по теоретическим разделам курса, реферат. Дополнительным средством оценки знаний и умений студентов является отчет о выполнении практических заданий и его защита.

По итогам курса обучающиеся сдают экзамен. Форма проведения – устный ответ с письменным подкреплением по утвержденным билетам, сформулированным с учетом содержания дисциплины. В билет для экзамена включается два теоретических вопроса и задача. В процессе подготовки к устному ответу студент должен составить в письменном виде план ответа.

2. Перечень компетенций с указанием этапов их формирования

При освоении дисциплины формируются следующие компетенцииПК-2 (индикаторы ПК-2.1), ПК-3 (индикаторы ПК-3.3).

Указанные компетенции формируются в соответствии со следующими этапами:

– формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работа студентов);

– приобретение и развитие практических умений предусмотренных компетенциями (практические занятия, самостоятельная работа студентов);

– закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, в ходе решения конкретных задач на занятиях, выполнения индивидуальных заданий на практических занятиях и их защиты, а так же в процессе сдачи экзамена.

3. Показатели и критерии оценивания компетенций (*результатов*) на различных этапах их формирования, описание шкал оценивания

Сформированность каждой компетенции в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

– пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

– продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

– эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

При достаточном качестве освоения более 80% приведенных знаний, умений и навыков преподаватель оценивает освоение данной компетенции в рамках настоящей дисциплины на эталонном уровне, при освоении более 60% приведенных знаний, умений и навыков – на продвинутом, при освоении более 40% приведенных знаний умений и навыков – на пороговом уровне. При освоении менее 40% приведенных знаний, умений и навыков компетенция в рамках настоящей дисциплины считается неосвоенной.

Уровень сформированности каждой компетенции на различных этапах ее формирования в процессе освоения данной дисциплины оценивается в ходе текущего контроля успеваемости и представлено различными видами оценочных средств.

Оценке сформированности в рамках данной дисциплины подлежат компетенции/индикаторы:

Показатели достижения планируемых результатов обучения и критерии их оценивания на разных уровнях формирования компетенций приведены в таблице 1.

Таблица 1. Показатели достижения индикаторов компетенции

1	2	3	4
Компетенция: код по ФГОС 3++, формулировка	**Индикаторы**	**Этап**	**Наименование оценочного средства**
ПК-2 (09.03.04/02 Программно-алгоритмическое обеспечение систем искусственного интеллекта) 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 - основные определения искусственного интеллекта и систем искусственного интеллекта, историю развития науки об искусственном интеллекте, эволюцию и главные тренды систем ИИ; классы решаемых задач с помощью СИИ; основные параметры идентификации задач ИИ; назначение, сфера применения, виды используемых знаний, временные аспекты решения задач УМЕТЬ - определять принадлежность проблемной и предметной областей	1	Зачет

1	2	3	4
	к классу решаемых задач с помощью систем ИИ и основные параметры идентификации задач СИИ ВЛАДЕТЬ - особенностями классификации и идентификации задач искусственного интеллекта для различных предметных областей.		
ПК-3 (09.03.04/02 Программно-алгоритмическое обеспечение систем искусственного интеллекта) Способен разрабатывать и тестировать программные компоненты решения задач в системах ИИ	**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.		

Преподавателем оценивается содержательная сторона и качество материалов, приведенных в отчетах студента по практическим занятиям. Кроме того, преподавателем учитываются ответы студента на вопросы по соответствующим видам занятий при текущем контроле:

– контрольные опросы;

– задания для практических занятий.

Принимается во внимание **знания** обучающимися:

- теоретических основ защиты информации;
- алгоритмов защиты информации и их практическая реализация;
- защиты программ от нелегального копирования;
- методов и алгоритмов сжатия данных.

умений:

- применять методы проектирования программного обеспечения и его программную реализацию;
- осуществлять сбор и обобщение информации о проблемной области путем опроса

экспертов, исходных данных о функционировании проблемной области, документированных источников знаний, а также формировать требования к системе искусственного интеллекта.

обладание навыками**:**

- реализации электронного аналога шифровальной машины «Энигма»;
- реализации алгоритма шифрования с открытым ключом (RSA);
- реализации алгоритма симметричного шифрования (AES);
- реализации алгоритма симметричного шифрования (DES)

Критерии оценивания уровня сформированности компетенции в процессе выполнения практических работ:

41%-60% правильных ответов соответствует пороговому уровню сформированности компетенции на данном этапе ее формирования;

61%-80% правильных ответов соответствует продвинутому уровню сформированности компетенции на данном этапе ее формирования;

81%-100% правильных ответов соответствует эталонному уровню сформированности компетенции на данном этапе ее формирования.

Сформированность уровня компетенций не ниже порогового является основанием для допуска обучающегося к промежуточной аттестации по данной дисциплине.

Формой промежуточной аттестации по данной дисциплине является зачет, оцениваемый по принятой в ФГБОУ ВО «РГРТУ» системе: «зачтено» и «не зачтено».

Критерии оценивания промежуточной аттестации представлены в таблице.

Шкала оценивания	Критерии оценивания
«зачтено»	**оценки «зачтено»** заслуживает обучающийся, продемонстрировавший полное знание материала изученной дисциплины, усвоивший основную литературу, рекомендованную рабочей программой дисциплины; выполнивший все практические задания; показавший систематический характер знаний по дисциплине, ответивший на все вопросы билета или допустивший погрешность в ответе вопросы, но обладающий необходимыми знаниями для их устранения под руководством преподавателя;
«не зачтено»	**оценки «не зачтено»** заслуживает обучающийся, не выполнивший практические задания, продемонстрировавший серьезные пробелы в знаниях основного материала изученной дисциплины, не ответивший на все вопросы билета и дополнительные вопросы. Оценка «не зачтено» ставится обучающимся, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине (формирования и развития компетенций, закрепленных за данной дисциплиной).

4. Типовые контрольные задания или иные материалы

ФОС по дисциплине содержит следующие оценочные средства, позволяющие оценить знания, умения и уровень приобретенных компетенций при текущем контроле и промежуточной аттестации, разбитые по модулям дисциплины:

- перечни экзаменационных вопросов;
- макеты билетов к экзамену.

Средства для оценки различных уровней формирования компетенций по категориям «знать», «уметь», «владеть» обеспечивают реализацию основных принципов контроля, таких, как объективность и независимость, практико-ориентированность, междисциплинарность.

С учетом этого, контрольные вопросы (задания, задачи,) входящие в ФОС, для различных категорий и уровней освоения компетенций имеют следующий вид:

Уровень ЗНАТЬ

Дескрипторы	Пример задания из оценочного средства
основные определения искусственного интеллекта и систем искусственного интеллекта, историю развития науки об искусственном интеллекте, эволюцию и главные тренды систем ИИ; классы решаемых задач с помощью СИИ; основные параметры идентификации задач ИИ; назначение, сфера применения, виды используемых знаний, временные аспекты решения задач	1. Дать определения следующих терминов: информация, защита информации, актив, информационная сфера, угроза, безопасность, информационная безопасность. 2. Перечислить модели доступа и описать особенности каждой из них. 3. Привести виды случайных чисел, и дать примеры алгоритмов их вычисления. Зачем нужны случайные числа.

Уровень УМЕТЬ

Дескрипторы	Пример задания из оценочного средства
определять принадлежность проблемной и предметной областей к классу решаемых задач с помощью систем ИИ и основные параметры идентификации задач СИИ	1. Дать определения следующих терминов: идентификация, авторизация, аутентификация. Дать примеры каждого из них. 2. Дать определение следующих терминов: шифрование, рассеивание. Требования к алгоритмам шифрования. Привести правила Керкхоффа.
проводить тестирование работоспособности и качества функционирования систем ИИ и проверять выполнение требований к системам ИИ со стороны пользователя	3. Привести алгоритм линейного конгруэнтного генератора. Какое распределение он дает? Какое распределение можно из него получить и с помощью какого преобразования?

Перечни вопросов к зачету

7 семестр

1. Какова цель моделирования угроз. Перечислить этапы моделирования угроз. Перечислить уровни возможности нарушителей. Дать определения термина угроза. Перечислить виды источников угроз.

2. Виды симметричного шифрования (поточные и блочные). Привести схему для одного из видов.

3. Какое шифрование называется симметричным? Описать алгоритм шифрования DES или AES.

4. Привести классификацию автоматизированных систем с точки зрения требований безопасности (3 класса защищенности). Перечислить подсистемы защиты

информации в автоматизированных системах.

5. Дать определения алгоритмов перестановки и подстановки. Привести примеры каждого из этих видов алгоритмов. Привести пример алгоритма, использующего оба подхода.

6. Дать определение асимметричного шифрования. Описать алгоритм шифрования RSA. Кто создает ключи: отправитель или получатель?

7. Дать определение одно- и многоалфавитных подстановок. К какому виду относится алгоритм Энигма. Привести схему алгоритма Энигма.

8. Описать алгоритм создания цифровой подписи. Описать алгоритм проверки цифровой подписи.

9. Дать определение электронной цифровой подписи. Дать определение электронного сертификата. Какие существуют модели организации инфраструктуры электронных сертификатов?

Перечень лабораторных работ

ЛР1.1 - ЛР1.2 Реализация электронного аналога шифровальной машины «Энигма».
Цель работы:
Разработка электронного аналога шифровальной машины.
Задание:

Реализовать в виде программы электронный аналог шифровальной машины «Энигма». Обеспечить шифрование и расшифровку произвольного файла с использованием разработанной программы. Предусмотреть работу программы с пустым, однобайтовым файлом. Программа также должна уметь обрабатывать файл архива (rar, zip или др.).

ЛР1.3 - ЛР2.1 Реализация алгоритма шифрования с открытым ключом (RSA).
Цель работы:
Разработка алгоритма шифрования с открытым ключом.
Задание:

Реализовать программу шифрования алгоритмом с открытым ключом. Использовать алгоритм RSA. Обеспечить шифрование и расшифровку произвольного файла с использованием разработанной программы. Предусмотреть работу программы с пустым, однобайтовым файлом. Программа также должна уметь обрабатывать файл архива (rar, zip или др.).

ЛР2.2 - ЛР2.3 Реализация алгоритма симметричного шифрования (DES).
Цель работы:
Разработка алгоритма симметричного шифрования (DES).
Задание:

Реализовать программу шифрования симметричным алгоритмом DES.Обеспечить шифрование и расшифровку произвольного файла с использованием разработанной программы. Предусмотреть работу программы с пустым, однобайтовым файлом. Программа также должна уметь обрабатывать файл архива (rar, zip или др.).

ЛР2.4 - ЛР3.1 Реализация алгоритма симметричного шифрования (AES).
Цель работы:
Разработка алгоритма симметричного шифрования (AES).
Задание:

Реализовать программу шифрования алгоритмом с открытым ключом. Использовать алгоритм RSA. Обеспечить шифрование и расшифровку произвольного файла с ис-

пользованием разработанной программы. Предусмотреть работу программы с пустым, однобайтовым файлом. Программа также должна уметь обрабатывать файл архива (rar, zipили др.).

ЛР3.2 - ЛР3.3 Создание и проверка электронной подписи для документа.
Цель работы:
Создание электронной подписи.
Задание:

Реализовать программу создания и проверки электронной подписи для документа. Обеспечить шифрование и расшифровку произвольного файла с использованием разработанной программы. Предусмотреть работу программы с пустым, однобайтовым файлом. Программа также должна уметь обрабатывать файл архива (rar, zip или др.).