МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»
Смоленский казачий институт промышленных технологий и бизнеса (филиал)

УТВЕРЖДАЮ
Председатель ПЦК
_____Максаков С. А.
«10» апреля 2026 г.

Рабочая программа дисциплины
МДК.02.02 Криптографические средства защиты информации

Закреплена за **ПЦК общепрофессиональных дисциплин; профессиональных модулей специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Специальность: **10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Направленность

на базе основного общего образования

Квалификация **техник по защите информации**

Форма обучения **очная**

Общая трудоемкость **160 часов**

Часов по учебному плану 160

в том числе:

контактная работа 146

самостоятельная работа 14

Виды контроля в семестрах:

Контрольная работа - 5,6

Распределение часов дисциплины по семестрам

Вид учебной работы	Трудоемкость, часов					
	семестр 5		**семестр 6**		Итого	
	УП	РП	УП	РП	УП	РП
Лекции	42	42	38	38	80	80
Лабораторные	14	14	20	20	34	34
Практические	14	14	18	18	32	32
В т.ч. в форме практ. подгот.	0	0	0	0	0	0
Контактная работа	70	70	76	76	146	146
Сам. работа	10	10	4	4	14	14
Часы на контроль						

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00F5 665F CCDB 5046 05DD 6E08 EBCB D00A DC
Действителен: с 21 октября 2025 г. по 14 января 2027 г.
Владелец: Коржикова Надежда Сергеевна
Должность: Директор

Москва, 2026

Программу составил:
Преподаватель Максаков Сергей Анатольевич _____

Рабочая программа дисциплины
Криптографические средства защиты информации

Разработана в соответствии с:
Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (приказ Минобрнауки России от 09.12.2016 г. № 1553)
06.033. Профессиональный стандарт "СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ", утверждённый приказом Министерства труда и социальной защиты Российско Федерации от 14 сентября 2022 г. N 525н (зарегистрирован Министерством юстиции Российской Федерации 14 октября 2022 г., регистрационный N 70543)

Разработана на основании учебного плана, утвержденного Учёным советом ФГБОУ ВО "МГУТУ им. К.Г. Разумовского (ПКУ)" от 26.03.2026 протокол №9.

СОДЕРЖАНИЕ

1. МЕСТО ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2. ЦЕЛИ, ЗАДАЧИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (УЧЕБНОГО ПРЕДМЕТА)

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	П

Дисциплина Криптографические средства защиты информации является частью неопознанный объект и обязательна для изучения.

Требования к предварительной подготовке обучающегося:	
1	Основы информационной безопасности
2	Математика

2. ЦЕЛИ, ЗАДАЧИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

Цели освоения: Формирование у студентов системы теоретических знаний и практических навыков в области применения криптографических методов и средств для обеспечения информационной безопасности автоматизированных систем, сетей и баз данных, а также выработка компетенций, необходимых для профессиональной деятельности по защите информации ограниченного доступа от несанкционированного доступа.
Задачи: 1. Сформировать у студентов системное понимание роли и места криптографических методов и средств в общей системе защиты информации.
2. Обеспечить усвоение теоретических основ криптографии, включая математический аппарат, классификацию криптоалгоритмов, протоколы и стандарты.
3. Развить практические навыки применения программных и программно-аппаратных средств криптографической защиты информации в профессиональной деятельности.
4. Подготовить студентов к самостоятельному решению задач по обеспечению информационной безопасности автоматизированных систем, сетей и баз данных.
5. Сформировать компетенции, необходимые для аттестации объектов информатизации по требованиям безопасности информации.
Изучение дисциплины направлено на формирование у обучающихся следующих компетенций:

ПК 2.4.: Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПК 2.4.1: Знать особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации
ПК 2.4.2: Уметь применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись
ПК 2.4.3: Иметь практический опыт решения задач защиты от несанкционированного доступа к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных

2.3	**Иметь практический опыт:**
2.3.1	ПК 2.1: Иметь навыки установки и настройки отдельных программных, программно-аппаратных средств защиты информации (ПАСЗИ).
2.3.2	ПК 2.2: Иметь навыки обеспечения защиты информации в автоматизированных системах с использованием отдельных программных, программно-аппаратных средств защиты информации (ПАСЗИ).
2.3.3	ПК 2.3: Иметь навыки тестирования функций отдельных программных и программно-аппаратных средств защиты информации (ПАСЗИ).
2.3.4	ПК 2.4: Иметь навыки обработки, хранения и передачи информации ограниченного доступа.
2.3.5	ПК 2.5: Иметь навыки уничтожения информации и носителей информации с использованием программных и программно-аппаратных средств.
2.3.6	ПК 2.6: Иметь навыки регистрации основных событий в автоматизированных (информационных) системах, включая использование средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов, тем и содержание занятий /вид занятия/	Семестр / Курс	Часов/ в том числе	Компетен-ции	Виды контроля
	1. РАЗДЕЛ 1. ОСНОВЫ КРИПТОГРАФИИ И МАТЕМАТИЧЕСКИЙ АППАРАТ				
1. 1	Тема 1.1. Введение в криптографию Определение криптографии, основные термины (шифр, ключ, шифротекст, открытый текст).	5	4/0	ПК 2.4.1	Устный опрос

	Классификация криптосистем. Принципы Керкгоффса. Модели нарушителей и угроз. Политика безопасности. Место криптографии в системе защиты информации. Знать: определение криптографии; базовые термины (открытый текст, шифротекст, ключ, шифр) и их взаимосвязь; классификацию криптосистем по типу ключа и по стойкости; принципы Керкгоффса; основные модели нарушителей и типы угроз; понятие политики безопасности как совокупности правил управления доступом и защиты данных /Лек/				
1. 2	Тема 1.2. Математические основы криптографии Теория чисел: НОД, алгоритм Евклида, сравнения по модулю, классы вычетов. Китайская теорема об остатках. Простые числа, тесты на простоту (Ферма, Миллера–Рабина). Функция Эйлера. Дискретное логарифмирование. Односторонние функции и их роль в криптографии. Знать: алгоритм Евклида для нахождения НОД и обратных элементов; свойства сравнений по модулю и операции с классами вычетов; китайскую теорему об остатках для решения систем модульных сравнений; определение простых чисел и вероятностные тесты на простоту; функцию Эйлера и её применение в вычислении показателя степени по модулю; постановку задачи дискретного логарифмирования как вычислительно сложной; определение односторонней функции и её ключевую роль как фундамента для построения асимметричных криптосистем, хеш-функций и протоколов цифровой подписи /Лек/	5	8/0	ПК 2.4.1	Устный опрос
1. 3	Практическая работа №1. Вычисление НОД, НОК и решение сравнений первой степени (алгоритм Евклида, расширенный алгоритм Евклида) Уметь: вычислять НОД классическим алгоритмом Евклида; находить НОК через формулу НОК(a,b) =|a·b|/НОД(a,b); применять расширенный алгоритм Евклида для получения коэффициентов Безу; решать линейные сравнения вида $a \cdot x \equiv b \pmod m$ через обратный элемент по модулю; определять наличие и количество решений по критерию НОД(a,m) | b. Владеть: навыками пошагового ручного выполнения алгоритма Евклида; техникой обратного хода расширенного алгоритма для вычисления коэффициентов; методом сокращения сравнения на общий делитель; навыками проверки решений подстановкой в исходное сравнение. /Пр/	5	2/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе
1. 4	Практическая работа №2. Применение китайской теоремы об остатках (решение систем сравнений, восстановление числа по модулям) Уметь: проверять условия совместности при попарно взаимно простых модулях; вычислять общий модуль и частичные произведения; находить обратные элементы по модулю с помощью расширенного алгоритма Евклида; восстанавливать решение системой подстановок или табличным методом; проверять решение подстановкой во все сравнения; адаптировать метод для непопарно взаимно простых модулей через сведение к эквивалентной системе.	5	2/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе

	Владеть: навыками пошагового применения КТО для систем из 2–4 сравнений; техникой модульных вычислений без калькулятора; методом проверки корректности восстановленного числа; интерпретацией результата как единственного класса вычетов по общему модулю. /Пр/				
1. 5	Самостоятельная работа по теме "Классификацию атак и модели нарушителей" /СР/	5	2/0	ПК 2.4.1,ПК 2.4.2,ПК 2.4.3	Вопросы для самоподготовки
	2. РАЗДЕЛ 2. КЛАССИЧЕСКИЕ И СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ КРИПТОАЛГОРИТМЫ				
2. 1	Тема 2.1. Классические шифры История криптографии. Шифры замены: одноалфавитные (Цезарь, Атбаш) и многоалфавитные (Виженер, Тритемий). Шифры перестановки: скитала, решётка Кардано, маршрутные шифры. Частотный криптоанализ. Стойкость классических шифров. Знать: основные этапы истории криптографии от древности до начала XX века; принципы шифров замены с их математическим описанием; принципы шифров перестановки; метод частотного криптоанализа для взлома одноалфавитных шифров на основе статистики языка; критерии стойкости классических шифров и их принципиальную уязвимость к атакам на открытый текст и частотному анализу /Лек/	5	6/0	ПК 2.4.1	Устный опрос
2. 2	Практическая работа №3. Ручное шифрование и дешифрование шифром Цезаря и Атбаш. Частотный анализ Уметь: шифровать и дешифровать тексты шифрами Цезаря (с заданным сдвигом) и Атбаш; подбирать неизвестный сдвиг методом перебора или по ключевым словам; строить частотную таблицу символов шифротекста; сопоставлять частоты с эталонными для языка; восстанавливать открытый текст одноалфавитной замены с учётом биграмм и триграмм. Владеть: навыками ручного шифрования по алфавитной таблице; методом частотного анализа как инструментом взлома; техникой подбора сдвига по пиковым символам; навыками выявления закономерностей (повторы, предлоги, окончания); умением интерпретировать результаты частотного распределения. /Пр/	5	2/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе
2. 3	Практическая работа №4. Шифрование и дешифрование шифром Виженера. Определение длины ключа Уметь: шифровать и дешифровать текст по таблице Виженера; определять длину ключа методами Касиски (по повторам) и индексом совпадений; восстанавливать ключ через частотный анализ по каждой позиции; применять тест Фридмана для оценки длины ключа. Владеть: навыками работы с таблицей Виженера; методом Касиски для обнаружения периода; вычислением индекса совпадений; разделением текста на группы по позициям ключа; частотным анализом для восстановления букв ключа; проверкой осмысленности восстановленного	5	2/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе

	ключа. /Пр/				
2. 4	Практическая работа №5. Шифры перестановки: построение маршрутных таблиц Уметь: строить маршрутные таблицы для заданного текста; шифровать записью по одному маршруту и считыванием по другому (змейка, спираль, строки, столбцы); дешифровать при известном маршруте и размерах; применять колончатую перестановку с ключевым словом; оценивать стойкость перестановок к статистическим атакам. Владеть: навыками построения таблиц разной размерности; техникой записи и считывания по траекториям; методом подбора размеров таблицы; восстановлением текста по известному маршруту; выявлением остаточных закономерностей в шифротексте. /Пр/	5	2/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе
2. 5	Лабораторная работа №1. Программная реализация шифров простой замены (Цезарь, Атбаш) с обработкой текстовых файлов Уметь: реализовывать шифрование/дешифрование Цезаря и Атбаш с учётом регистра и небуквенных символов; читать текст из файла и записывать результат; реализовывать подбор сдвига перебором или по частотам; обрабатывать ошибки ввода-вывода; тестировать на разных текстах. Владеть: навыками программирования алгоритмов замены; работой с файловым вводом-выводом; отладкой криптографического кода; организацией алфавитных строк и функций сдвига; обработкой краевых случаев (пустой файл, кодировка, пробелы). /Лаб/	5	4/0	ПК 2.4.2,ПК 2.4.3	Отчёт по лабораторной работе
2. 6	Лабораторная работа №2. Программная реализация шифра Виженера и частотного криптоанализа (автоматическое определение ключа) Уметь: реализовывать шифрование/дешифрование Виженера с заданным ключом; автоматически определять длину ключа методами индекса совпадений и Касиски; восстанавливать ключ частотным анализом по каждой позиции; выполнять полное дешифрование без известного ключа; обрабатывать тексты на русском и английском; оценивать точность восстановления в зависимости от длины текста. Владеть: навыками программирования многоалфавитных шифров; реализацией индекса совпадений; группировкой символов по позициям ключа; частотным анализом для восстановления букв; тестированием на разных текстах; оптимизацией переборных алгоритмов. /Лаб/	5	6/0	ПК 2.4.2,ПК 2.4.3	Отчёт по лабораторной работе
2. 7	Тема 2.2. Поточные шифры и генераторы ПСЧ Принцип поточного шифрования. Генераторы псевдослучайных чисел: линейный конгруэнтный, BBS, Фибоначчи. Режим гаммирования. Алгоритм RC4: структура, инициализация, генерация ключевого потока. Достоинства, недостатки и уязвимости поточных шифров. Знать: принцип поточного шифрования как побитового (побайтового) наложения ключевого потока (гаммы) на открытый текст с	5	6/0	ПК 2.4.1	Устный опрос

	использованием операции XOR; классификацию генераторов псевдослучайных чисел и их криптографическую пригодность; режим гаммирования как синхронный или самосинхронизирующийся потоковый процесс; архитектуру алгоритма RC4; достоинства поточных шифров и недостатки /Лек/				
2. 8	Лабораторная работа №3. Реализация генератора ПСЧ и режима гаммирования (шифрование/дешифрование файлов) Уметь: реализовывать генератор ПСЧ (LCG, BBS или LFSR) с задаваемыми параметрами; реализовывать режим гаммирования через XOR для файлов любого размера; обеспечивать синхронизацию генератора при шифровании и дешифровании; инициализировать генератор от пароля или ключа; обрабатывать текстовые и бинарные файлы; добавлять вектор инициализации для защиты от повторного использования гаммы. Владеть: навыками программирования генераторов ПСЧ; техникой побайтового XOR-шифрования; работой с бинарными файлами; синхронизацией состояния генератора; потоковой обработкой больших файлов без загрузки в память; тестированием случайности выходной последовательности. /Лаб/	5	4/0	ПК 2.4.2,ПК 2.4.3	Отчёт по лабораторной работе
2. 9	Тема 2.3. Блочные симметричные шифры Архитектура блочных шифров: сеть Фейстеля (DES, ГОСТ 28147-89) и SP-сеть (AES, «Кузнечик»). Режимы шифрования: ECB, CBC, CFB, OFB, CTR (назначение, сильные и слабые стороны). Отечественные стандарты: ГОСТ 28147 -89, «Магма», «Кузнечик» (ГОСТ Р 34.12-2015). Зарубежные: DES, 3DES, AES. Сравнительный анализ. Знать: архитектуры Фейстеля (DES, ГОСТ 28147-89) и SP-сети (AES, «Кузнечик»); режимы шифрования (ECB, CBC, CFB, OFB, CTR) с их сильными и слабыми сторонами; отечественные стандарты («Магма», «Кузнечик» по ГОСТ Р 34.12 -2015); зарубежные алгоритмы (DES, 3DES, AES); сравнительный анализ по размеру блока, ключу, раундам, стойкости и области применения. /Лек/	5	10/0	ПК 2.4.1	Устный опрос
2. 10	Практическая работа №6. Анализ режимов шифрования блочных алгоритмов (ECB vs CBC) – сравнение визуальных различий на примере изображений Уметь: шифровать растровые изображения в режимах ECB и CBC на AES или ГОСТ; дешифровать и сравнивать с оригиналом; визуально выявлять артефакты (сохранение контуров в ECB, шум в CBC); объяснять причины сохранения паттернов в ECB; генерировать тестовые изображения с однородными областями; сравнивать производительность режимов; рекомендовать выбор режима по типу данных. Владеть: навыками работы с графическими и криптографическими библиотеками; техникой поблочного шифрования в разных режимах; методом визуального сравнения; интерпретацией артефактов; документированием выводов о стойкости и применимости режимов. /Пр/	5	2/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе

2. 11	Самостоятельная работа "Отечественные и зарубежные стандарты шифрования" /СР/	5	4/0	ПК 2.4.1,ПК 2.4.2,ПК 2.4.3	Вопросы для самоподготовки
	3. РАЗДЕЛ 3. АСИММЕТРИЧНАЯ КРИПТОГРАФИЯ				
3. 1	Тема 3.1. Криптосистемы с открытым ключом Основы асимметричной криптографии. Распределение ключей: проблема Диффи-Хеллмана. Алгоритм Диффи–Хеллмана (обмен ключами). Алгоритм RSA: генерация ключевой пары, функции шифрования и расшифрования, цифровая подпись на основе RSA. Знать: принцип асимметричной криптографии; проблему распределения ключей и протокол Диффи–Хеллмана для выработки общего секрета по открытому каналу; алгоритм RSA /Лек/	5	8/0	ПК 2.4.1	Устный опрос
3. 2	Практическая работа №7. Ручной расчёт RSA (выбор простых чисел, вычисление открытой и закрытой экспоненты, шифрование и расшифрование чисел) Уметь: выбирать простые p и q для ручного расчёта; вычислять модуль n и функцию Эйлера φ (n); выбирать e, взаимно простую с φ(n); вычислять d как обратный элемент к e по модулю φ(n) через расширенный алгоритм Евклида; шифровать и расшифровывать числа возведением в степень по модулю; проверять корректность через тождество $d \cdot e \equiv 1 \bmod \varphi(n)$. Владеть: навыками ручного возведения в степень по модулю; техникой расширенного алгоритма Евклида для нахождения обратного элемента; проверкой взаимной простоты e и φ(n); расчётами для чисел до 1000; проверкой ключевой пары; интерпретацией как демонстрации асимметричной криптографии. /Пр/	5	2/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе
3. 3	Самостоятельная работа по теме "Сравнение симметричной и асимметричной криптографии" /СР/	5	2/0	ПК 2.4.1,ПК 2.4.2,ПК 2.4.3	Вопросы для самоподготовки
	4. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ (5 СЕМЕСТР)				
4. 1	Контрольная работа ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа /К/	5	2/0	ПК 2.4.1,ПК 2.4.2,ПК 2.4.3	Вопросы для контрольной работы
	5. РАЗДЕЛ 4. КРИПТОГРАФИЧЕСКИЕ ХЕШ-ФУНКЦИИ				
5. 1	Тема 4.1. Хеш-функции Понятие хеш-функции. Требования к криптографическим хеш-функциям: односторонность, устойчивость к коллизиям, лавинный эффект. Обзор алгоритмов: MD5, SHA-1, SHA-2 (256/512), SHA-3. Отечественный стандарт ГОСТ Р 34.11-2012 («Стрибог»). Применение хешей для контроля целостности, хранения паролей, совместно с ЭЦП. Атаки на хеш-функции. Знать: определение хеш-функции; три требования (односторонность, стойкость к коллизиям,	6	8/0	ПК 2.4.1	Устный опрос

	лавинный эффект); обзор алгоритмов (MD5, SHA-1, SHA-2, SHA-3, ГОСТ Р 34.11-2012 «Стрибог»); применения (целостность, пароли, ЭЦП); основные атаки (коллизии, предобразы, «день рождения») /Лек/				
5. 2	Практическая работа №8. Криптографические хеш-функции Уметь: вычислять хеши алгоритмами MD5, SHA-1, SHA-256, SHA-512, ГОСТ Р 34.11-2012; демонстрировать лавинный эффект при изменении одного символа; проверять целостность файлов по контрольным суммам; генерировать соль и хешировать пароль с солью; различать алгоритмы по длине и стойкости (MD5/SHA-1 — скомпрометированы, SHA-2/Стрибог — стойкие). Владеть: навыками работы с утилитами и библиотеками хеширования; методом проверки лавинного эффекта; техникой хеширования паролей с солью; выбором алгоритма по задаче; документированием сравнения по скорости и стойкости. /Пр/	6	4/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе
5. 3	Лабораторная работа №4. Программная реализация хеш-функции (на примере MD5 или упрощённой версии SHA-256) Уметь: реализовывать алгоритм хеширования с побитовыми операциями; выполнять дополнение сообщения до кратности блоку; инициализировать буферы константами; реализовывать функции сжатия (раунды, сдвиги, сложения); обрабатывать данные блоками; сверять результат с эталонными тестовыми векторами; выполнять потоковое хеширование файлов. Владеть: навыками побитового программирования; работой с 32-битными целыми; реализацией циклических сдвигов и логических операций; пошаговой отладкой раундов; сверкой с эталонами; обработкой больших файлов блочным чтением; документированием реализации. /Лаб/	6	6/4	ПК 2.4.2,ПК 2.4.3	Отчёт по лабораторной работе
	6. РАЗДЕЛ 5. ЭЛЕКТРОННАЯ ПОДПИСЬ И ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ				
6. 1	Тема 5.1. Электронная подпись (ЭП) Понятие и юридическая сила ЭП. Свойства: целостность, аутентичность, неотказуемость. Схемы ЭП на основе RSA и DSA. Отечественный стандарт ГОСТ Р 34.10-2012 (на основе эллиптических кривых). Коды аутентификации сообщений (MAC) на основе симметричных ключей. Сравнение MAC и ЭП. Применение в электронном документообороте, СКЗИ. Знать: понятие и юридическую силу ЭП; три свойства (целостность, аутентичность, неотказуемость); схемы RSA и DSA; отечественный ГОСТ Р 34.10-2012 на эллиптических кривых; MAC на симметричных ключах; сравнение MAC (без неотказуемости, быстрее) и ЭП (с неотказуемостью, медленнее); применение в документообороте и СКЗИ. /Лек/	6	10/0	ПК 2.4.1	Устный опрос
6. 2	Практическая работа №9. Работа с сертифицированным СКЗИ для ЭП (генерация ключей, подписание документа, проверка)	6	4/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе

	Уметь: устанавливать и настраивать сертифицированное СКЗИ (КриптоПро CSP, ViPNet CSP); генерировать ключевую пару в защищённом контейнере на токене; формировать запрос на сертификат и импортировать полученный сертификат; подписывать документ (отсоединённая/присоединённая подпись) по ГОСТ Р 34.10-2012; проверять подпись по сертификату; различать форматы ЭП (CAdES-BES, CAdES-T); устранять типовые ошибки. Владеть: навыками установки лицензии и настройки криптопровайдера; техникой генерации контейнеров на Рутокен или JaCarta; подписанием через интерфейс или командную строку (cryptcp); проверкой подписи и сертификата; работой с аппаратными токенами и драйверами; интерпретацией результатов проверки и документированием. /Пр/				
6. 3	Лабораторная работа №5. Программная реализация схемы ЭП на основе RSA (генерация подписи и верификация) Уметь: программно генерировать ключевую пару RSA; создавать подпись хешированием сообщения и возведением в степень закрытой экспоненты; верифицировать подпись возведением в открытую степень и сравнением с хешем; использовать хеширование для сообщений произвольной длины; преобразовывать хеш в число; проверять корректность на тестовых данных; обрабатывать ошибки несовпадения. Владеть: навыками программирования RSA; работой с большими числами (BigInteger); модульным возведением в степень; хешированием перед подписанием; отладкой по тестовым векторам; обработкой ошибок; оформлением отчёта с примерами. /Лаб/	6	8/0	ПК 2.4.2,ПК 2.4.3	Отчёт по лабораторной работе
6. 4	Тема 5.2. Идентификация и аутентификация Базовые понятия. Протоколы аутентификации: на основе паролей (в том числе стойкое хеширование), одноразовых паролей (OTP). Криптографические протоколы: CHAP, EAP. Протокол Kerberos (билеты, TGT). Многофакторная аутентификация. Атаки на системы аутентификации. Знать: понятия идентификации и аутентификации; парольные протоколы (с солью) и OTP; CHAP и EAP; Kerberos (билеты, TGT, KDC); многофакторность; основные атаки (подбор, перехват, повтор, фишинг, кража токенов). /Лек/	6	6/0	ПК 2.4.1	Устный опрос
6. 5	Практическая работа №10. Анализ протоколов аутентификации (сравнение парольных, токенных и криптографических протоколов) Уметь: классифицировать протоколы по факторам (знание, владение, биометрия); сравнивать парольные (передача, хеширование, соль), OTP (TOTP, HOTP) и криптографические (CHAP, EAP, Kerberos) по стойкости и защите от атак; оценивать применимость для разных сценариев; выявлять уязвимости и предлагать улучшения. Владеть: навыками составления сравнительных таблиц (стойкость, удобство, скорость, затраты); анализом потоков сообщений; интерпретацией угроз; обоснованием выбора по модели	6	4/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе

	нарушителя; документированием рекомендаций. /Пр/				
6. 6	Лабораторная работа №6. Разработка прототипа системы аутентификации (регистрация, хеширование пароля, вход) Уметь: разрабатывать приложение с регистрацией и входом; хешировать пароли с солью алгоритмами bcrypt, Argon2 или PBKDF2; генерировать уникальную соль и сохранять с хешем; проверять пароль при входе через хеш с солью; обрабатывать ошибки; защищать от перебора (задержки, лимит попыток); тестировать устойчивость к подбору. Владеть: навыками работы с БД или файловым хранилищем; генерацией криптостойкой соли; безопасным сравнением хешей; отладкой и логированием; документированием архитектуры и обоснованием выбора алгоритмов. /Лаб/	6	6/0	ПК 2.4.2,ПК 2.4.3	Отчёт по лабораторной работе
6. 7	Самостоятельная работа по теме "Биометрические методы". /СР/	6	2/0	ПК 2.4.1,ПК 2.4.2,ПК 2.4.3	Вопросы для самоподготовки
	7. РАЗДЕЛ 6. ПРИКЛАДНЫЕ АСПЕКТЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ				
7. 1	Тема 6.1. Защита информации в сетях и базах данных Криптографическая защита сетевых соединений: стек протоколов SSL/TLS (рукопожатие, сертификаты, шифрование сессии). IPSec (AH, ESP, IKE). Защита беспроводных сетей WPA2/WPA3. Шифрование баз данных: на уровне столбцов, таблиц, дисков (TDE – Transparent Data Encryption). СКЗИ и их интеграция с СУБД. Знать: защиту сетевых соединений через SSL/TLS (рукопожатие, сертификаты, сессионное шифрование) и IPSec (AH, ESP, IKE); защиту беспроводных сетей WPA2/WPA3; шифрование БД на уровнях столбцов, таблиц и дисков (TDE); интеграцию СКЗИ с СУБД. /Лек/	6	8/0	ПК 2.4.1	Устный опрос
7. 2	Практическая работа №11. Настройка защищённого соединения SSL/TLS (веб-сервер, анализ сертификатов, проверка шифров) Уметь: настраивать веб-сервер (Apache/Nginx) с SSL/TLS; генерировать самоподписанный сертификат или CSR; отключать устаревшие протоколы (SSLv2/v3, TLS 1.0/1.1); выбирать безопасные шифры; проверять сертификат и цепочку доверия через openssl s_client или браузер; анализировать параметры соединения; применять усиление TLS (HSTS). Владеть: навыками работы с OpenSSL (генерация ключей, CSR, сертификатов); правкой конфигов веб-сервера для HTTPS; проверкой через openssl s_client; интерпретацией предупреждений браузера; документированием конфигурации по рекомендациям Mozilla. /Пр/	6	4/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе
7. 3	Тема 6.2. Организационные аспекты. Аттестация объектов информатизации Классификация СКЗИ по уровням защиты. Сертификация и лицензирование в области криптозащиты. Установка и настройка СКЗИ (порядок действий). Проверка выполнения требований по защите от НСД при аттестации	6	6/0	ПК 2.4.1	Устный опрос

	объектов информатизации. Документы, регламентирующие аттестацию. Оформление результатов. Знать: классификацию СКЗИ по уровням защиты; порядок сертификации и лицензирования криптосредств; этапы установки и настройки СКЗИ; проверку требований по защите от НСД при аттестации; основные регламентирующие документы и оформление результатов аттестации. /Лек/				
7. 4	Практическая работа №12. Разработка проекта аттестационной документации (составление перечня проверяемых требований, актов проверки) Уметь: составлять перечень проверяемых требований по нормативным документам (ФСТЭК); разрабатывать программу испытаний; оформлять акты проверки защиты от НСД; формировать заключение о соответствии; выявлять несоответствия и давать рекомендации; структурировать пакет аттестационной документации. Владеть: навыками работы с нормативной базой; составлением чек-листов по классам защищённости; оформлением актов и заключений; аргументацией выводов о готовности; планированием мероприятий по устранению замечаний. /Пр/	6	2/0	ПК 2.4.2,ПК 2.4.3	Отчёт по практической работе
	8. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ (6 СЕМЕСТР)				
8. 1	Контрольная работа ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа /К/	6	2/0	ПК 2.4.1,ПК 2.4.2,ПК 2.4.3	Вопросы для контрольной работы, итоговое тестирование

Список выбранных образовательный технологий:

Название	Описание
Информационные технологии	Личностно ориентированная технология, способ организации самостоятельной деятельности учащихся, направленный на решение задачи учебного проекта
Кейс-технология	Технология включает в себя: индивидуальную самостоятельную работу обучаемых с материалами кейса (идентификация проблемы, формулирование ключевых альтернатив, предложение решения или рекомендуемого действия); работу в малых группах по согласованию видения ключевой проблемы и ее решений; презентацию и экспертизу результатов малых групп на общей дискуссии (в
Технология модульного обучения	Технология модульного обучения основана на идее личностно-ориентированного подхода. Основной технологии модульного обучения является самостоятельное освоение учебных дисциплин, которые для удобства поделены на модули. Цель технологии модульного обучения – создать условия выбора для полного овладения содержанием образовательных программ в разной

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ

Оценочные средства текущего контроля успеваемости:

ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

РАЗДЕЛ 1. ОСНОВЫ КРИПТОГРАФИИ И МАТЕМАТИЧЕСКИЙ АППАРАТ

Тема 1.1. Введение в криптографию
1. Что такое криптография и какова её основная цель в информационной безопасности?
2. В чем заключаются фундаментальные отличия между криптографией и стеганографией?
3. Какие основные задачи решаются с помощью криптографических методов?
4. Что представляет собой модель Керкгоффса и почему она считается основополагающей в современной криптографии?
5. Как классифицируются криптографические алгоритмы по типу используемых ключей?
6. Каковы основные этапы эволюции криптографии от древности до наших дней?

7. Что такое криптоанализ и какие существуют типы атак на шифры (атака на основе только шифротекста, с известным открытым текстом и т.д.)?
8. В чем разница между понятиями «стойкость шифра» и «вычислительная сложность взлома»?
9. Какую роль играют случайные числа и энтропия в построении криптостойких систем?
10. Каковы основные правовые и этические аспекты использования криптографии в РФ?

Тема 1.2. Математические основы криптографии
1. Какие основные алгебраические структуры (группы, кольца, поля) используются в криптографии и в чем их различие?
2. В чем суть алгоритма Евклида и как расширенный алгоритм Евклида применяется для нахождения обратного элемента по модулю?
3. Что такое функция Эйлера (φ(n)) и как она используется в теореме Эйлера для модульной арифметики?
4. Какие существуют тесты простоты чисел (детерминированные и вероятностные) и для чего они нужны?
5. В чем заключается дискретное логарифмирование и почему эта задача считается сложной (вычислительно трудной)?
6. Что такое конечные поля (поля Галуа — GF) и каково их значение для построения S-блоков в блочных шифрах?
7. Как работают основные поразрядные логические операции (XOR, AND, OR, сдвиги), используемые в криптоалгоритмах?
8. Каковы свойства простых чисел и факторизации, лежащие в основе асимметричных криптосистем?
9. В чем отличие операций сложения и умножения в конечном поле GF(2^n) от операций в поле целых чисел?
10. Как вычисляется наибольший общий делитель (НОД) для больших чисел и как это связано с криптостойкостью?

РАЗДЕЛ 2. КЛАССИЧЕСКИЕ И СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ КРИПТОАЛГОРИТМЫ

Тема 2.1. Классические шифры
1. В чем принципиальная разница между шифрами замены (подстановки) и перестановки (транспозиции)?
2. Как работает шифр Цезаря и каким образом его можно модифицировать для увеличения стойкости (аффинный шифр)?
3. Что такое шифр Виженера и в чем заключается его уязвимость к атаке на основе повторяющихся ключевых последовательностей?
4. Каков принцип работы шифра Плейфера и для чего используется биграммный анализ?
5. Как работает шифр Хилла на основе матричного умножения и какое условие необходимо для его обратимости?
6. Что представляют собой шифры перестановки (маршрутное чтение, вертикальная перестановка) и как они взламываются?
7. Каковы основные методы криптоанализа классических шифров (частотный анализ, метод Касиски)?
8. Почему классические шифры считаются нестойкими к атакам с использованием современных вычислительных мощностей?
9. Как работает машина «Энигма» и какой принцип шифрования в ней использовался?
10. В чем заключается отличие одноалфавитных шифров от многоалфавитных и как это влияет на сложность взлома?

Тема 2.2. Поточные шифры и генераторы ПСЧ
1. В чем заключается основное отличие поточных шифров от блочных с точки зрения способа обработки данных?
2. Как работает генератор псевдослучайных чисел (ПСЧ) на основе регистра сдвига с линейной обратной связью (РСЛОС / LFSR)?
3. Что такое инициализирующий вектор (IV) и какова его роль в поточных шифрах для предотвращения повторного использования ключевого потока?
4. Почему для поточных шифров критически важно никогда не использовать одну и ту же ключевую последовательность (one-time pad) дважды?
5. Какие атаки возможны на поточные шифры при повторном использовании ключевого потока (атака на основе XOR)?
6. В чем различие между синхронными и самосинхронизирующимися поточными шифрами?
7. Какие существуют современные стандарты поточного шифрования (например, RC4, Salsa20/ChaCha20) и в чем их особенности?
8. Какие требования предъявляются к криптографически стойким генераторам случайных чисел (ГСЧ / RNG)?
9. Как энтропия источника влияет на качество генерируемых ключей в ПСЧ?
10. В чем заключается атака на основе корреляции и как она применяется к поточным шифрам на основе РСЛОС?

Тема 2.3. Блочные симметричные шифры
1. Каковы основные режимы работы блочных шифров (ECB, CBC, CFB, OFB, CTR) и в чем их ключевые различия?
2. Почему режим ECB (Electronic Codebook) считается небезопасным для шифрования данных, превышающих размер одного блока?
3. Что такое сеть Фейстеля и каков принцип ее работы на примере шифра DES?
4. Какие основные операции выполняются в алгоритме AES (Rijndael) на этапах SubBytes, ShiftRows, MixColumns и AddRoundKey?
5. Как осуществляется процесс формирования раундовых ключей (Key Schedule) в блочных шифрах?
6. В чем отличие алгоритмов шифрования DES и 3DES (Triple DES) и почему был принят стандарт AES?
7. Что такое S-блоки (таблицы замен) и P-блоки (перестановки) и как они обеспечивают свойства конфузии и диффузии?
8. Как работает атака «встреча посередине» (Meet-in-the-Middle) и против каких шифров она эффективна?
9. В чем суть атак на основе подобранных открытых текстов и адаптивных подобранных открытых текстов на блочные шифры?

10. Каковы основные преимущества и недостатки шифрования в режиме сцепления блоков (CBC) по сравнению с режимом счетчика (CTR)?

РАЗДЕЛ 3. АСИММЕТРИЧНАЯ КРИПТОГРАФИЯ

Тема 3.1. Криптосистемы с открытым ключом
1. В чем заключается основная концепция асимметричной криптографии и почему она решает проблему распределения ключей?
2. Как работает алгоритм RSA и на каких математических задачах строится его стойкость (факторизация)?
3. В чем суть алгоритма Диффи-Хеллмана (DH) и как он позволяет двум сторонам согласовать общий секретный ключ по незащищенному каналу?
4. На чем основана стойкость криптосистемы Эль-Гамаля и какая математическая задача лежит в ее основе (дискретное логарифмирование)?
5. Каковы основные этапы генерации ключевой пары (открытый и закрытый ключи) в алгоритме RSA?
6. Что такое эллиптические кривые (ECC) и почему криптография на их основе считается более эффективной по сравнению с RSA при том же уровне стойкости?
7. Какие практические задачи, помимо шифрования, решаются с помощью асимметричных алгоритмов (цифровая подпись, обмен ключами)?
8. В чем заключается проблема аутентичности открытых ключей и как она решается с помощью инфраструктуры открытых ключей (PKI) и сертификатов?
9. Какие существуют основные типы атак на асимметричные криптосистемы (атака на основе подобранного шифротекста, факторизация, квантовые алгоритмы)?
10. В чем различие между гибридной криптосистемой и использованием только асимметричного шифрования для больших объемов данных?

РАЗДЕЛ 4. КРИПТОГРАФИЧЕСКИЕ ХЕШ-ФУНКЦИИ

Тема 4.1. Хеш-функции
1. Какие основные свойства должна удовлетворять криптографическая хеш-функция (детерминизм, устойчивость к коллизиям, лавинный эффект)?
2. В чем разница между понятиями «устойчивость к коллизиям первого рода» (прообраз) и «второго рода» (второй прообраз)?
3. Для каких целей используются хеш-функции в информационной безопасности (контроль целостности, хранение паролей, ЭЦП)?
4. Каков принцип работы алгоритмов MD5 и SHA-1 и почему в настоящее время они считаются небезопасными?
5. Чем отличаются хеш-функции семейства SHA-2 от SHA-3 с точки зрения внутренней структуры (конструкция Меркла-Дамгора против конструкции губки)?
6. Что такое «парадокс дней рождения» и как он используется для оценки вероятности коллизий в хеш-функциях?
7. Как работает атака «длина-расширение» (length extension attack) и против каких хеш-функций она применима?
8. Что такое соль (salt) и для чего она используется при хешировании паролей для защиты от радужных таблиц?
9. В чем заключается отличие криптографической хеш-функции от обычной хеш-таблицы или контрольной суммы (CRC)?
10. Какие существуют российские стандарты хеширования (ГОСТ Р 34.11-2012 / Стрибог) и каковы их параметры?

РАЗДЕЛ 5. ЭЛЕКТРОННАЯ ПОДПИСЬ И ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ

Тема 5.1. Электронная подпись (ЭП)
1. Что такое электронная подпись и какие три основных свойства она должна обеспечивать (целостность, аутентичность, неотказуемость)?
2. В чем отличие между простой электронной подписью и усиленной квалифицированной электронной подписью (КЭП) согласно 63-ФЗ?
3. Как работает алгоритм создания и проверки цифровой подписи на основе RSA или ECDSA?
4. Что такое хеш-код документа и какова его роль в формировании электронной подписи?
5. В чем суть схемы цифровой подписи Эль-Гамаля и каковы ее математические основы?
6. Что представляет собой сертификат ключа проверки электронной подписи и кто является удостоверяющим центром (УЦ)?
7. Какие атаки возможны на системы электронной подписи (подделка подписи, атака на хеш-функцию, компрометация закрытого ключа)?
8. В чем отличие подписи с восстановлением сообщения от подписи с приложением сообщения?
9. Как осуществляется проверка срока действия сертификата и его статус (CRL, OCSP) при верификации подписи?
10. Каковы особенности использования электронной подписи в корпоративных системах документооборота (СЭД)?

Тема 5.2. Идентификация и аутентификация
1. В чем разница между процессами идентификации, аутентификации и авторизации субъекта доступа?
2. Какие существуют основные факторы аутентификации (по знанию, по владению, по свойству) и их комбинации (двухфакторная аутентификация)?
3. Как работают протоколы аутентификации на основе паролей и каковы основные уязвимости этого подхода?
4. Что такое одноразовые пароли (OTP) и какие алгоритмы их генерации существуют (TOTP, HOTP)?

5. Как работает протокол аутентификации «запрос-ответ» (Challenge-Response) и каким образом он защищает от атак повторного воспроизведения (Replay attacks)?
6. Какие протоколы аутентификации используются в сети Интернет (Kerberos, RADIUS, DIAMETER) и в чем их особенности?
7. Что такое биометрическая аутентификация и каковы ее основные проблемы (ложный отказ, ложный пропуск, невозможность смены биометрического шаблона)?
8. Как протокол Диффи-Хеллмана может быть использован для взаимной аутентификации сторон?
9. В чем заключается концепция единого входа (Single Sign-On — SSO) и какие протоколы (SAML, OAuth) для этого используются?
10. Каковы основные правила безопасности при организации системы аутентификации в корпоративной сети (политика паролей, блокировки, аудит)?

РАЗДЕЛ 6. ПРИКЛАДНЫЕ АСПЕКТЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Тема 6.1. Защита информации в сетях и базах данных
1. Какие криптографические протоколы используются для защиты каналов связи (SSL/TLS, IPSec) и в чем их различие?
2. Как работает протокол TLS при установлении безопасного соединения (рукопожатие) и как в нем сочетаются симметричное и асимметричное шифрование?
3. Какие существуют подходы к шифрованию данных в базах данных (прозрачное шифрование на уровне диска, шифрование столбцов, шифрование на уровне приложения)?
4. В чем заключаются проблемы поиска по зашифрованным данным в СУБД и как они решаются (порядковое шифрование, гомоморфное шифрование)?
5. Какие типы VPN-соединений существуют и какие криптографические алгоритмы в них применяются?
6. Как обеспечивается безопасность электронной почты с использованием протоколов S/MIME и PGP/GPG?
7. Что такое защищенный канал и какие угрозы (прослушивание, подмена, разрыв) он должен нейтрализовать?
8. Каковы особенности защиты данных в облачных хранилищах и кто отвечает за управление ключами (BYOK, HYOK)?
9. Как работает технология токенизации и чем она отличается от шифрования применительно к защите данных платежных карт?
10. Какие существуют методы защиты от атак по побочным каналам (Side-channel attacks) в сетевых устройствах?

Тема 6.2. Организационные аспекты. Аттестация объектов информатизации
1. Что такое объект информатизации (ОИ) и какие этапы включает его аттестация по требованиям безопасности информации?
2. Какова роль организационно-распорядительных документов (политик безопасности) в системе криптографической защиты?
3. Какие нормативные документы (ГОСТ, приказы ФСБ, ФСТЭК) регламентируют использование криптографических средств в РФ?
4. Что входит в понятие «система защиты информации» (СЗИ) объекта информатизации и как криптография в нее встраивается?
5. Каков порядок классификации автоматизированной системы (АС) по уровню значимости обрабатываемой информации?
6. Что такое сертификация средств криптографической защиты информации (СКЗИ) и почему обязательно использование только сертифицированных средств для госорганов?
7. Какие основные этапы проводятся при проведении специальной проверки объекта информатизации на предмет отсутствия недекларированных возможностей?
8. Как организован процесс управления ключевой информацией (жизненный цикл ключей: генерация, хранение, распределение, уничтожение) в организации?
9. Какие меры организационного характера необходимы для предотвращения инсайдерских угроз при работе с шифровальными средствами?
10. В чем заключается суть аудита информационной безопасности и как проверяется соответствие аттестованному классу защищенности объекта?

ВОПРОСЫ ДЛЯ САМОПОДГОТОВКИ

Самостоятельная работа по теме "Классификацию атак и модели нарушителей"
1. По какому основному критерию криптографические атаки делятся на пассивные и активные, и чем они отличаются с точки зрения воздействия на систему?
2. Какие три фундаментальных свойства информационной безопасности (CIA — конфиденциальность, целостность, доступность) нарушаются при атаках типа «Перехват», «Модификация», «Фабрикация» и «Прерывание обслуживания»?
3. Что такое атака «человек посередине» (Man-in-the-Middle) и на каких этапах криптографического обмена она может быть реализована?
4. Какие существуют классы атак по типу доступа злоумышленника к шифруемым данным (атака на основе только шифротекста, с известным открытым текстом, с подобранным открытым текстом и адаптивная)?
5. Как классифицируются нарушители информационной безопасности по уровню полномочий и исходному доступу к объекту информатизации согласно нормативным документам ФСТЭК России?
6. В чем принципиальное отличие внешнего нарушителя от внутреннего, и какие стартовые возможности есть у каждой из этих категорий?
7. Какие виды атак относятся к категории «криптоанализ на основе побочных каналов» (атаки по времени выполнения,

по энергопотреблению, по электромагнитному излучению) и против каких криптоалгоритмов они эффективны?
8. Что такое атаки повторного воспроизведения (Replay attacks) и какие протокольные механизмы (временные метки, одноразовые номера nonce) используются для защиты от них?
9. Какие модели нарушителей выделяются в зависимости от наличия у них специальных технических средств (СТС) для перехвата информации и доступа к средствам криптографической защиты информации (СКЗИ)?
10. Как классифицируются атаки по месту их реализации (локальные, удаленные, внутрисетевые, межсетевые) и какое это имеет значение для выбора организационных мер противодействия?

Самостоятельная работа "Отечественные и зарубежные стандарты шифрования"
1. Какие основные российские стандарты шифрования регламентируются ГОСТ Р 34.12–2015 и какие алгоритмы в них определены?
2. В чем заключаются ключевые отличия между отечественным блочным шифром «Кузнечик» и зарубежным стандартом AES?
3. Каковы параметры алгоритма «Магма» (размер блока, длина ключа, количество раундов) и какая архитектура в нем используется?
4. Какие стандарты NIST (США) определяют алгоритмы симметричного шифрования, хеширования и электронной подписи?
5. В чем различие между сетью Фейстеля (ГОСТ «Магма») и SP-сетью (AES, «Кузнечик») с точки зрения преобразования данных?
6. Какие российские стандарты регламентируют криптографические хеш-функции (ГОСТ Р 34.11) и электронную подпись (ГОСТ Р 34.10)?
7. В чем отличие российского стандарта хеширования «Стрибог» от зарубежных SHA-2 и SHA-3 по размеру выходного хеша и внутренней структуре?
8. Какой зарубежный стандарт определяет алгоритм электронной подписи на основе эллиптических кривых (ECDSA) и в чем его отличие от российского ГОСТ Р 34.10–2012?
9. Какие режимы работы блочных шифров закреплены в ГОСТ Р 34.13–2015 и чем они отличаются от режимов, определенных в стандартах NIST?
10. Какие существуют нормативные и организационные проблемы при интеграции российских и зарубежных криптостандартов в единых информационных системах, и как они решаются?

Самостоятельная работа по теме "Сравнение симметричной и асимметричной криптографии"
1. В чем заключается принципиальное различие между симметричной и асимметричной криптографией с точки зрения используемых ключей?
2. Какие задачи информационной безопасности решаются с помощью симметричных криптоалгоритмов, а какие — с помощью асимметричных?
3. Каковы основные преимущества и недостатки симметричной криптографии по сравнению с асимметричной в вопросах скорости шифрования?
4. В чем состоит проблема распределения ключей в симметричной криптографии и как асимметричная криптография решает эту проблему?
5. Какие математические задачи лежат в основе стойкости асимметричных алгоритмов (факторизация, дискретное логарифмирование) и почему они считаются вычислительно сложными?
6. Как обеспечивается конфиденциальность, целостность, аутентичность и неотказуемость в симметричных и асимметричных системах?
7. В чем заключается концепция гибридной криптосистемы и почему она широко применяется на практике (например, в протоколе TLS)?
8. Каковы требования к длине ключа в симметричной и асимметричной криптографии для обеспечения одинакового уровня стойкости (сравнение 128-битного симметричного ключа и 3072-битного RSA)?
9. Какие существуют основные типы атак, характерные для симметричных алгоритмов, и какие — для асимметричных?
10. В чем состоит угроза квантовых вычислений для симметричных и асимметричных криптосистем (алгоритмы Гровера и Шора)?

Самостоятельная работа по теме "Биометрические методы".
1. Что такое биометрическая аутентификация и какие основные физиологические и поведенческие биометрические характеристики человека используются для идентификации?
2. В чем отличие биометрической аутентификации от традиционных методов (по паролю, по токену) с точки зрения факторов аутентификации?
3. Каковы основные этапы работы биометрической системы (регистрация, извлечение шаблона, сравнение, принятие решения)?
4. Что такое FAR (False Acceptance Rate) и FRR (False Rejection Rate), в чем их взаимосвязь и почему они являются ключевыми показателями эффективности биометрической системы?
5. В чем заключается основная проблема биометрических методов с точки зрения компрометации (невозможность замены биометрического шаблона) и как она решается с помощью криптографических методов?
6. Какие биометрические методы считаются наиболее надежными (по FAR/FRR) и почему — например, отпечатки пальцев, радужная оболочка глаза, голос, геометрия лица?
7. Что такое «обход биометрической системы» (спуфинг) и какие существуют способы защиты от подделки биометрических образцов (например, liveness detection)?
8. Какие криптографические методы используются для защиты биометрических шаблонов в базах данных (хеширование, шифрование, гомоморфное шифрование, биокриптосистемы)?

9. В чем заключается отличие между режимами идентификации (один ко многим, 1:N) и верификации (один к одному, 1:1) в биометрических системах?
10. Каковы правовые и этические ограничения при сборе, хранении и обработке биометрических данных согласно законодательству РФ (например, 152-ФЗ «О персональных данных»)?

Практические и лабораторные работы см в Приложение А

Оценочные средства промежуточной аттестации:
см. Приложение Б
Темы индивидуальных проектов, курсовых работ (проектов), индивидуальных заданий на практику:
Учебным планом не предусмотрено

Описание критериев оценивания успеваемости

НЕДОСТАТОЧНЫЙ УРОВЕНЬ	ПОРОГОВЫЙ УРОВЕНЬ	ПРОДВИНУТЫЙ УРОВЕНЬ	ВЫСОКИЙ УРОВЕНЬ
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала; - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам; - незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «незачет», «неудовлетворительно»	Оценка «зачтено/удовлетворительно» ,«удовлетворительно»	Оценка «зачтено/хорошо», «хорошо»	Оценка «зачтено/отлично», «отлично»

ПК 2.4.: Осуществлять обработку, хранение и передачу информации ограниченного доступа

Недостаточный уровень:
Знает отдельные названия СЗИ (антивирус, брандмауэр, пароль), понимает различие между идентификацией и аутентификацией (кто ты / докажи), знает 1-2 криптографических метода (шифрование, хэширование), а также знает, что такое управление доступом (права).

Умеет под руководством преподавателя назначать право на чтение/запись пользователю в БД, выполнять простую проверку прав по инструкции, шифровать строку с помощью онлайн-утилиты, а также подписывать документ ЭП по образцу.

Имеет практический опыт создания учётной записи и назначения базовых прав по инструкции, генерации ключевой пары ЭП с помощью утилиты под контролем, шифрования файла симметричным ключом (паролем) по образцу, а также проверки целостности файла с помощью хэш-функции по шаблону.

Пороговый уровень:
Знает особенности и способы применения программных и программно-аппаратных СЗИ в операционных системах (политики безопасности, контроль учётных записей, аудит, шифрование дисков), компьютерных сетях

Знает особенности и способы применения программных и программно-аппаратных СЗИ в операционных системах (политики безопасности, контроль учётных записей, аудит, шифрование дисков), компьютерных сетях (межсетевые экраны, VPN, IDS/IPS, сегментация), базах данных (разграничение доступа на уровне таблиц/строк/столбцов, шифрование, аудит запросов); типовые модели управления доступом (дискреционная (DAC), мандатная (MAC), ролевая (RBAC), атрибутная (ABAC)); средства, методы и протоколы идентификации и аутентификации (парольная, двухфакторная, биометрическая, сертификатная; протоколы: PAP, CHAP, Kerberos, RADIUS, TACACS+, OAuth, SAML); основные понятия криптографии (шифрование, дешифрование, ключ, хэш-функция, ЭП, сертификат, PKI); типовые криптографические методы и средства защиты информации (симметричное шифрование (AES, ГОСТ), асимметричное шифрование (RSA, ГОСТ), хэширование (MD5, SHA, ГОСТ), электронная подпись, шифрование дисков, VPN на базе IPsec/OpenVPN, СКЗИ).

Умеет самостоятельно применять средства защиты БД (назначение прав доступа на таблицы/строки/столбцы, шифрование столбцов, включение аудита запросов), проверять выполнение требований по защите от НСД при аттестации объектов информатизации (проверка настроек СЗИ в БД, анализ журналов, тестирование на простые атаки (SQL-инъекции)), применять математический аппарат для криптографических преобразований (выполнять арифметические операции в конечных полях, рассчитывать простые числа, хэш-функции), а также использовать типовые программные криптографические средства (СКЗИ: шифрование данных, вычисление хэша; настройка электронной подписи (генерация ключевой пары, подпись, проверка подписи)).

Имеет практический опыт решения задач защиты от НСД: настройки разграничения доступа в ОС (DAC/RBAC), настройки антивируса и брандмауэра, шифрования дисков и файлов (BitLocker/LUKS/VeraCrypt), настройки VPN; применения электронной подписи (генерация ключевой пары, подпись, проверка, работа с сертификатами); применения симметричных (AES/ГОСТ, режимы) и асимметричных (RSA/ГОСТ, шифрование, обмен ключами) криптоалгоритмов; использования средств шифрования (СКЗИ: КриптоПро, OpenSSL, GnuPG, шифрование БД, дисков, сетевых соединений); а также документирования выполненных мер защиты.

Продвинутый уровень:
Знает детальные особенности применения СЗИ для различных классов защищённости, модели управления доступом в специализированных ОС (Astra Linux, SELinux), методы усиления аутентификации (FIDO2, WebAuthn, PKI с аппаратными токенами), криптографические алгоритмы с точки зрения стойкости (длины ключей, режимы шифрования), а также требования нормативных документов (ФСТЭК, ФСБ) к СЗИ, моделям доступа и криптографии.

Умеет самостоятельно настраивать защиту БД для различных СУБД (MS SQL, PostgreSQL, Oracle, MySQL) с учётом требований ФСТЭК, проводить углублённую проверку защищённости при аттестации (пентест БД, анализ уязвимостей), применять математический аппарат для реализации криптографических алгоритмов (AES, RSA, ГОСТ), а также настраивать сертифицированные СКЗИ (КриптоПро, ViPNet) и интегрировать ЭП в приложения.

Имеет практический опыт проектирования и настройки комплексной защиты от НСД для различных ОС (Astra Linux, Windows, Linux) и классов защищённости (ФСТЭК), применения квалифицированной ЭП в корпоративных системах (интеграция с 1С, ЭДО), выбора и настройки криптоалгоритмов с учётом стойкости (длины ключей, режимы), а также настройки сертифицированных СКЗИ (КриптоПро, ViPNet) для защиты данных на дисках, в БД и в сети.

Высокий уровень:
Знает методологию построения комплексных систем защиты с учётом моделей доступа и криптографии, современные протоколы аутентификации (Zero Trust, непрерывная аутентификация), квантово-стойкие криптографические алгоритмы, постквантовую криптографию, а также стратегии интеграции криптографических методов в гетерогенных и распределённых средах.

Умеет самостоятельно проектировать комплексную защиту БД с интеграцией в SIEM и DLP, автоматизировать аттестационные проверки, применять постквантовые криптографические алгоритмы, разрабатывать стратегии использования ЭП в распределённых системах (блокчейн, смарт-контракты), интерпретировать требования регуляторов (ФСТЭК, ФСБ), а также обучать других защите БД, аттестации, криптографии и использованию ЭП.

Имеет практический опыт внедрения систем защиты от НСД в гетерогенных и распределённых средах (Zero Trust, микросегментация, EDR), применения постквантовых криптоалгоритмов, интегрирования ЭП с блокчейн и смарт-контрактами, использования гибридной криптографии и квантово-стойких решения, а также обучения других защите от НСД, применению ЭП, симметричных/асимметричных алгоритмов и средств шифрования.

Перечень практических навыков, приобретаемых при изучении дисциплины:

ПК 2.1: Иметь навыки установки и настройки отдельных программных, программно-аппаратных средств защиты информации (ПАСЗИ).
ПК 2.2: Иметь навыки обеспечения защиты информации в автоматизированных системах с использованием отдельных программных, программно-аппаратных средств защиты информации (ПАСЗИ).
ПК 2.3: Иметь навыки тестирования функций отдельных программных и программно-аппаратных средств защиты информации (ПАСЗИ).
ПК 2.4: Иметь навыки обработки, хранения и передачи информации ограниченного доступа.
ПК 2.5: Иметь навыки уничтожения информации и носителей информации с использованием программных и программно-аппаратных средств.
ПК 2.6: Иметь навыки регистрации основных событий в автоматизированных (информационных) системах, включая использование средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Методы оценки	Критерии оценки
Экспертное наблюдение за решением обучающимися проблемно-ситуационных задач в рамках практической подготовки	Оценка «отлично» – задание выполнено полностью, в рамках регламента, установленного на публичную презентацию, студент(ы) приводит (подготовили) полную четкую аргументацию выбранного решения на основе качественно сделанного анализа задания. Демонстрируются хорошие теоретические знания, имеется собственная обоснованная точка зрения на проблему(ы) и причины ее (их) возникновения. В случае ряда выявленных проблем четко определяет их иерархию. При устной презентации уверенно и быстро отвечает на заданные вопросы, выступление сопровождается приемами визуализации. В случае письменного отчета-презентации по выполнению кейс-задания сделан структурированный и детализированный анализ, представлены возможные варианты решения (3-5), четко и аргументировано обоснован окончательный выбор одного из альтернативных решений. Оценка «хорошо» – задание выполнено полностью, но в рамках установленного на выступление регламента, студент(ы) не приводит (не подготовили) полную четкую аргументацию выбранного решения. Имеет место излишнее теоретизирование, или наоборот, теоретическое обоснование ограничено, имеется собственная точка зрения на проблемы, но не все причины ее возникновения установлены. При устной презентации на дополнительные вопросы выступающий отвечает с некоторым затруднением, подготовленная устная презентации выполненного задания не очень структурирована. При письменном отчете-презентации по выполнению задания сделан неполный анализ, без учета ряда фактов, выявлены не все возможные проблемы, для решения могла быть выбрана второстепенная, а не главная проблема, количество представленных возможных вариантов решения – 2-3, затруднена четкая аргументация окончательного выбора одного из альтернативных решений. Оценка «удовлетворительно» – задание выполнено более чем на 2/3, но в рамках установленного на выступление регламента, студент(ы) расплывчато раскрывает решение, не может четко аргументировать сделанный выбор, показывает явный недостаток теоретических знаний. Выводы слабые, свидетельствуют о недостаточном анализе фактов, в основе решения может иметь место интерпретация фактов или предположения, собственная точка зрения на причины возникновения проблемы не обоснована или отсутствует. При устной презентации на вопросы отвечает с трудом или не отвечает совсем. Подготовленная презентация выполненного задания не структурирована. В случае письменной презентации по выполнению кейсзадания не сделан детальный анализ, далеко не все факты учтены, для решения выбрана второстепенная, а не главная проблема, количество представленных возможных вариантов решения – 1-2, отсутствует четкая аргументация окончательного выбора решения. Оценка «неудовлетворительно» – задание не выполнено, или выполнено менее чем на треть. Отсутствует детализация при анализе задания, изложение устное или письменное не структурировано. Если решение и обозначено в выступлении или отчете-презентации, то оно не является решением проблемы, которая заложена в задании.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Рекомендуемая литература

5.1.1. Основная литература

Л.1.1	Бабаш А.В., Баранова Е.К. Криптографические методы и средства защиты информации [Электронный ресурс]:Учебник. - Москва: КноРус, 2024. - 222 с. – Режим доступа: https://book.ru/book/950118
Л.1.2	Рацеев С. М. Криптографические протоколы. Схемы разделения секрета [Электронный ресурс]:учебное пособие для вузов. - Санкт-Петербург: Лань, 2024. - 336 с. – Режим доступа: https://e.lanbook.com/book/367457
Л.1.3	Гисин В. Б. Криптография и распределенные реестры [Электронный ресурс]:учебное пособие. - Москва: Прометей, 2022. - 186 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=700941
Л.1.4	Бабаш А.В., Баранова Е.К. Криптографические методы защиты информации [Электронный ресурс]:Учебник. - Москва: КноРус, 2024. - 189 с. – Режим доступа: https://book.ru/book/949929
Л.1.5	Никифоров С. Н. Методы защиты информации. Пароли, скрытие, шифрование [Электронный ресурс]:учебное пособие для вузов. - Санкт-Петербург: Лань, 2023. - 124 с. – Режим доступа: https://e.lanbook.com/book/338018
Л.1.6	Никифоров С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2022. - 160 с. – Режим доступа: https://e.lanbook.com/book/206285
Л.1.7	Никифоров С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2022. - 160 с. – Режим доступа: https://e.lanbook.com/book/224672

5.1.2. Дополнительная литература

Л.2.1	Никифоров С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2019. - 160 с. – Режим доступа: https://e.lanbook.com/book/114699

Л.2.2	Никифоров С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2020. - 160 с. – Режим доступа: https://e.lanbook.com/book/146803
Л.2.3	Никифоров С. Н. Методы защиты информации. Пароли, скрытие, шифрование [Электронный ресурс]:учебное пособие для вузов. - Санкт-Петербург: Лань, 2020. - 124 с. – Режим доступа: https://e.lanbook.com/book/146885
Л.2.4	Никифоров С. Н. Методы защиты информации. Пароли, скрытие, шифрование [Электронный ресурс]:. - Санкт-Петербург: Лань, 2021. - 124 с. – Режим доступа: https://e.lanbook.com/book/173803
Л.2.5	Трипкош В. А., Матвеев А. Г. Электронная цифровая подпись в деятельности предприятий и организаций [Электронный ресурс]:учебное пособие. - Оренбург: Оренбургский государственный университет, 2012. - 172 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=270314

5.2. Перечень программного обеспечения

Microsoft Visual Studio Professional 2017

5.3. Перечень информационных справочных систем

Электронно-библиотечная система "Лань"
Научная электронная библиотека "eLIBRARY.RU"
ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ»

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1312 - Лаборатория Учебная аудитория для проведения занятий лекционного типа, лабораторных и практических занятий; занятий семинарского типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Маркерная доска; 15 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Учебно-наглядные пособия

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Методические рекомендации по организации самостоятельной работы

СРС – планируемая учебная, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (возможно частичное непосредственное участие преподавателя при сохранении ведущей роли студентов). Целью СРС является овладение фундаментальными знаниями, профессиональными умениями и навыками по профилю будущей специальности, опытом творческой, исследовательской деятельности, развитие самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровней. Задачи СРС: систематизация и закрепление полученных теоретических знаний и практических умений студентов; углубление и расширение теоретической подготовки; формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу; развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности; формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации; развитие исследовательских умений; использование материала, собранного и полученного в ходе самостоятельных занятий на практических занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к текущей и промежуточной аттестации. Функции СРС: развивающая (повышение культуры умственного труда, приобщение к 10 творческим видам деятельности, обогащение интеллектуальных способностей студентов); информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится мало результативной); ориентирующая и стимулирующая (процессу обучения придается ускорение и мотивация); воспитательная (формируются и развиваются профессиональные качества специалиста и гражданина); исследовательская (новый уровень профессионально-творческого мышления).

Самостоятельная работа студентов является обязательным компонентом учебного процесса для каждого студента и определяется учебным планом. Самостоятельная работа определяется как индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем. Самостоятельная работа – это познавательная учебная деятельность, когда последовательность мышления студента, его умственных и практических операций и действий зависит и определяется самим студентом.

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня, что в итоге приводит к развитию навыка самостоятельного планирования и реализации деятельности. Целью самостоятельной работы студентов является овладение необходимыми компетенциями по своему направлению подготовки, опытом творческой и исследовательской деятельности. На основании компетентностного подхода к реализации профессиональных образовательных программ, видами заданий для самостоятельной работы являются:

- для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы), составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа, использование аудио- и видеозаписей, компьютерной техники и информационно-телекоммуникационной сети Интернет и др.
- для закрепления и систематизации знаний: работа с конспектом лекции, обработка текста (учебника, первоисточника, дополнительной литературы, аудио и видеозаписей), повторная работа над учебным материалом, составление плана, составление таблиц для систематизации учебного материала, ответ на контрольные вопросы, заполнение рабочей тетради, аналитическая обработка текста (аннотирование, рецензирование, реферирование, конспект-анализ и др.), завершение аудиторных практических работ и оформление отчётов по ним, подготовка мультимедиа

сообщений/докладов к выступлению на семинаре (конференции), материалов-презентаций, подготовка реферата, составление библиографии, тематических кроссвордов, тестирование и др.
- для формирования умений: решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, выполнение расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, рефлексивный анализ профессиональных умений с использованием аудио- и видеотехники и др.
Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Методические рекомендации по освоению дисциплины (учебного предмета)

Методические рекомендации по подготовке к лекционным занятиям

Просмотрите конспект сразу после занятий. Пометьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю. Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.
Работа с рекомендованной литературой:
При работе с основной и дополнительной литературой целесообразно придерживаться такой последовательности. Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом. Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать. План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала. Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов:
- план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения,
- текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника,
- свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом,
- тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу. В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

Методические рекомендации по подготовке к практическим занятиям

Практические занятия представляют особую форму сочетания теории и практики. Их назначение – углубление проработки теоретического материала предмета путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к практическим занятиям включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение практического занятия предполагает, например:
- индивидуальные выступления студентов с сообщениями по какому-либо вопросу изучаемой темы;
- фронтальное обсуждение рассматриваемой проблемы, обобщения и выводы;
- решение задач и упражнений по образцу;
- решение вариантных задач и упражнений;
- решение ситуационных производственных (профессиональных) задач;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности.
- выполнение контрольных работ;
- работу с тестами.

При подготовке к практическим занятиям студентам рекомендуется: внимательно ознакомиться с тематикой практического занятия; прочесть конспект лекции по теме, изучить рекомендованную литературу;
составить краткий план ответа на каждый вопрос практического занятия; проверить свои знания, отвечая на вопросы для самопроверки; если встретятся незнакомые термины, обязательно обратиться к словарю и зафиксировать их в тетради. Все письменные задания выполнять в рабочей тетради. Практические занятия развивают у студентов навыки самостоятельной работы по решению конкретных задач.

Методические рекомендации по подготовке к лабораторным работам

Лабораторные работы представляют одну из форм освоения теоретического материала с одновременным формированием практических навыков в изучаемой дисциплине. Их назначение – углубление проработки теоретического материала, формирование практических навыков путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к лабораторным работам включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение лабораторной работы предполагает:
- изучение теоретического материала по теме лабораторной работы (по вопросам изучаемой темы);
- выполнение необходимых расчетов и экспериментов;

 оформление отчета с заполнением необходимых таблиц, построением графиков, подготовкой выводов по проделанным экспериментам и теоретическим расчетам;
 по каждой лабораторной работе проводится контроль: проверяется содержание отчета, проверяется усвоение теоретического материала. Контроль усвоения теоретического материала является индивидуальным.

Методические указания по выполнению отчёта к лабораторным работам

Основным требованием по выполнению лабораторных и практических работ является полное исчерпывающее описание всей проделанной работы, позволяющее судить о полученных результатах, степени выполнения и профессиональной подготовки студентов.
Методические указания обеспечивают комплексный подход в учебной работе студентов, единство и преемственность требований к оформлению результатов работы на разных этапах обучения. С единых позиций приведены основные требования по структуре, оформлению и содержанию отчета по лабораторным и практическим работам.
Структура отчёта:
- цель работы;
- краткие теоретические сведения;
- ход выполнения работы;
- выводы.
Дополнительными элементы:
- приложения;
- библиографический список.
Требования к содержанию отчёта:
1. Титульный лист
В верхнем поле листа указывают полное наименование учебного заведения.
В среднем поле указывается вид работы, в данном случае лабораторная или практическая работа с указанием курса, по которому она выполнена, и ниже ее название. Название работы приводится без слова тема и в кавычки не заключается.
Далее ближе к правому краю титульного листа указывают фамилию, инициалы и группу учащегося, выполнившего работу, а также фамилию, инициалы преподавателя, принявшего работу.
В нижнем поле листа указывается место выполнения работы и год ее написания (без слова год).
2. Цель работы должна отражать тему работы, а также конкретные задачи, поставленные студенту на период выполнения работы. По объему цель работы в зависимости от сложности и многозадачности работы составляет от нескольких строк до 0,5 страницы.
3. Краткие теоретические сведения. В этом разделе излагается краткое теоретическое описание изучаемой в работе темы. Материал раздела не должен копировать содержание методического пособия или учебника по данной теме, а ограничивается изложением основных понятий, требующихся для дальнейшей обработки полученных результатов. Объем литературного обзора не должен превышать 1/3 части всего отчета.
4. Ход выполнения работы. В данном разделе подробно излагается методика выполнения работы, процесс получения данных и способ их обработки. Если используются стандартные пакеты компьютерных программ для обработки экспериментальных результатов, то необходимо обосновать возможность и целесообразность их применения, а также подробности обработки данных с их помощью.
5. Выводы по работе - кратко излагаются результаты работы, полученные в результате выполнения работы, а также краткий анализ полученных результатов.
Для защиты лабораторной работы студент должен подготовить отчет, провести самостоятельную работу, иметь отметку о проверенном отчете.
Результаты определяются по пятибалльной системе оценок.

Методические рекомендации по выполнению реферата

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы. Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора. Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и для каких целей их использует. Требования к языку реферата.
Должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата:
1. Титульный лист
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты,

представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных. Общие требования к построению, содержанию и оформлению».
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

Методические рекомендации по устному опросу/самоподготовке

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, используя лист опорных сигналов, воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств. В случае необходимости следует рекомендовать еще раз внимательно разобраться в материале. Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение решать задачи или пройти тестирование по пройденному материалу. Однако преподавателю следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

Методические рекомендации по подготовке к семинарским занятиям

Одним из видов внеаудиторной самостоятельной работы является подготовка к семинарским занятиям. Семинар – форма учебно-практических занятий, при которой студенты обсуждают сообщения, доклады и рефераты, выполненные ими по результатам учебных или научных исследований под руководством преподавателя. Преподаватель в этом случае является координатором обсуждений темы семинара, подготовка к которому является обязательной. Поэтому тема семинара и основные источники обсуждения предъявляются до обсуждения для детального ознакомления, изучения. Цели обсуждений направлены на формирование навыков профессиональной полемики и закрепление обсуждаемого материала. Семинар – это такая форма организации обучения, при которой на этапе подготовки доминирует самостоятельная работа учащихся с
учебной литературой и другими дидактическими средствами над серией вопросов, проблем и задач, а в процессе семинара идут активное обсуждение, дискуссии и выступления учащихся, где они под руководством преподавателя делают обобщающие выводы и заключения. Семинар предназначен для углубленного изучения дисциплины, овладения методологией научного познания, то главная цель семинарских занятий – обеспечить студентам возможность овладеть навыками и умениями использования теоретического знания применительно к особенностям изучаемой отрасли.

Методические рекомендации по подготовке эссе

Одним из видов самостоятельной работы студентов является написание творческой работы по заданной либо согласованной с преподавателем теме. Творческая работа (эссе) представляет собой оригинальное произведение объемом 500-700 слов, посвященное какой-либо значимой классической либо современной проблеме в определенной теоретической и практической области. Творческая работа не является рефератом и не должна носить описательный характер, большое место в ней должно быть уделено аргументированному представлению своей точки зрения студентами, критической оценке рассматриваемого материала и проблематики, что должно способствовать раскрытию творческих и аналитических способностей. Цели написания эссе – научиться логически верно и аргументировано строить устную и письменную речь;
работать над углублением и систематизацией своих философских знаний; овладеть способностью использовать основы знаний для формирования мировоззренческой позиции. Приступая к написанию эссе, изложите в одном предложении, что именно вы будете утверждать и доказывать (свой тезис).

Методические рекомендации по подготовке к докладу

Для подготовки доклада необходимо выбрать актуальную тему. Желательно, чтобы тема была интересна докладчику и вызывала желание качественно подготовить материалы. Подготовка доклада предполагает: определение цели доклада; подбор необходимого материала, определяющего содержание доклада; составление плана доклада, распределение собранного материала в необходимой логической последовательности.
Композиция доклада имеет вступление, основную часть и заключение.
Вступление должно содержать: название доклада; сообщение основной идеи; современную оценку предмета изложения; краткое перечисление рассматриваемых вопросов; интересную для слушателей форму изложения. Основная часть, в которой необходимо раскрыть суть темы, обычно строится по принципу отчёта. Задача основной части: представить достаточно данных для того, чтобы слушатели заинтересовались темой.
Заключение – чёткое обобщение и краткие выводы по излагаемой теме.

Методические рекомендации по подготовке к собеседованию

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы,

связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.
Цель собеседования: проверка усвоения знаний; умений применять знания; сформированности профессионально значимых личностных качеств.
Подготовка к собеседованию предполагает повторение пройденного материала и приобретение навыка свободного владения терминологией и фактическими данными по определенному разделу дисциплины.

Методические рекомендации по подготовке к тестированию/ итоговому тестированию

Тестирование/итоговое тестирование – это система стандартизированных заданий, определенного содержания и упорядоченных в рамках определенной стратегии предъявления, позволяющая качественно оценить структуру и эффективно измерить уровень знаний, умений и навыков по учебной дисциплине (разделу). Тестирование/итоговое тестирование позволяет оценить у студентов уровень знаний фактического материала, умения логически мыслить, способности к рефлексии и творческому подходу к решению поставленной задачи на каждом этапе их обучения.
При самостоятельной подготовке к тестированию/итоговому тестированию студенту необходимо:
- четко выяснить все условия тестирования/итогового тестирования заранее (сколько тестов будет предложено, сколько времени отводится на тестирование/итоговое тестирование, какова система оценки результатов);
- проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- проработать информационный материал по разделу дисциплине;
- конспективно выписать из соответствующих разделов учебной дисциплины основные понятия, ключевые идеи, теоретические концепции и подходы;
- повторить теоретический материал лекций, самостоятельно изученной учебной и научной литературы, семинарских занятий.
При выполнении тестовых заданий рекомендуется:
- внимательно полностью прочитать вопрос и предлагаемые варианты ответов, выбрать правильные из них (их может быть несколько);
- при затруднении при ответе на сложный для студента вопрос целесообразно переходить к другим вопросам теста. По завершению ответов на все последующие вопросы теста необходимо вернуться к трудному вопросу и дать на него продуманный ответ;
- по окончании тестирования/итогового тестирования следует проверить правильность данных ответов на вопросы теста, чтобы избежать механических ошибок.

Методические рекомендации по подготовке к экзамену

Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине. Экзаменационная сессия – это серия экзаменов, установленных учебным планом. Между экзаменами интервал 2-4 дня, в течение студент систематизирует уже имеющиеся знания. На консультации перед экзаменом студенты должны
быть ознакомлены с основными требованиями и получить ответы на возникающие в процессе подготовки вопросы. Необходимо ориентировать студентов на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для систематизации знаний.

Методические рекомендации по подготовке к зачету/ зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно- методической документацией:
- программой дисциплины;
- перечнем знаний, умений и навыков, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.
После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета/зачета с оценкой.

Методические рекомендации по выполнению курсовой работы/ курсового проекта

Курсовая работа/курсовой проект - это учебно-исследовательский труд студента, выполняемый по определённой дисциплине под руководством научного руководителя. Её цель - закрепить и углубить теоретические знания, развить навыки самостоятельного анализа, работы с научной литературой и эмпирическими данными, а также сформировать умения структурировать информацию и формулировать обоснованные выводы.
Курсовая работа/курсовой проект – письменная работа объемом 30–50 страниц, выполняется в несколько этапов:
1. Подготовительный этап
2. Сбор и анализ информации
3. Написание работы
Структура курсовой работы/курсового проекта:
1. Титульный лист – по шаблону вуза.

2. Содержание – разделы с номерами страниц.
3. Введение: актуальность, цель, задачи, объект, предмет, методы, значимость, структура.
4. Основная часть:
о Глава 1 (теоретическая) – анализ концепций, выводы.
о Глава 2 (аналитическая/практическая) – анализ объекта, расчёты, данные, выводы.
о Глава 3 (рекомендательная, если нужно) – предложения, прогнозы, выводы.
5. Заключение – выводы по задачам, итоги, перспективы.
6. Список литературы – группируйте по типам, оформляйте по ГОСТ, указывайте только использованные источники.
7. Приложения (если нужно) – таблицы, графики, анкеты и т. д. (нумеруются, есть ссылки в тексте).
4. Оформление
5. Проверка и доработка
6. Подготовка к защите
• Доклад (5–7 мин.):
• Презентация.

Методические рекомендации по подготовке к зачету/ зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно- методической документацией:
- программой дисциплины;
- перечнем знаний, умений и навыков, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.
После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета/зачета с оценкой.

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.
Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей.
Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.
Основной формой в дистанционном обучении является индивидуальная форма обучения. Главным достоинством индивидуального обучения для инвалидов и лиц с ограниченными возможностями здоровья является то, что оно позволяет полностью индивидуализировать содержание, методы и темпы учебной деятельности инвалида, следить за каждым его действием и операцией при решении конкретных задач; вносить вовремя необходимые коррекции как в деятельность студента-инвалида, так и в деятельность преподавателя. Дистанционное обучение также обеспечивает возможности коммуникаций не только с преподавателем, но и с другими обучаемыми, сотрудничество в процессе познавательной деятельности.
При изучении дисциплины используются следующие организационные мероприятия:

- использование возможностей сети «Интернет» для обеспечения связи с обучающимися, предоставления им необходимых материалов для самостоятельного изучения, контроля текущей успеваемости и проведения тестирования;

- проведение видеоконференций, лекций, консультаций, и т.д. с использованием программ, обеспечивающих дистанционный контакт с обучающимся в режиме реального времени.
- предоставление электронных учебных пособий, включающих в себя основной материал по дисциплинам, включенным в ОП;

- проведение занятий, консультаций, защит курсовых работ и т.д. на базе консультационных пунктов, обеспечивающих условия для доступа туда лицам с ограниченными возможностями;
- предоставление видеолекций, позволяющих изучать материал курса дистанционно.
- использование программного обеспечения и технических средств, имеющих функции адаптации для использования лицами с ограниченными возможностями.

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2026 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2027 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2028 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2029 г. № __
Председатель ПЦК _____

==========

ПРИЛОЖЕНИЕ А

ЗАДАНИЯ НА ПРАКТИЧЕСКИЕ РАБОТЫ

Практическая работа №1

Тема: Вычисление НОД, НОК и решение сравнений первой степени (алгоритм Евклида, расширенный алгоритм Евклида)

Задание 1. Проверка условия взаимной простоты (криптографическая значимость)

Даны два числа: p (кандидат в простой модуль) и e (кандидат в открытую экспоненту).

Используя алгоритм Евклида, найдите НОД(p,e). На основании полученного результата сделайте вывод: допустима ли данная пара для использования в схеме RSA (напомним, что для RSA необходимо, чтобы НОД(e,$\varphi(n)$)=1)?

Задание 2. Вычисление закрытой экспоненты (расширенный алгоритм Евклида)

Для пары чисел (e,φ), где φφ – функция Эйлера, найдите мультипликативный обратный элемент $d=e^{-1} \bmod \varphi$.

Результат (d) является секретной экспонентой в RSA. Обязательно выполните проверку: $(e \cdot d) \bmod \varphi = 1$.

Задание 3. Решение сравнений для криптоанализа (или восстановления сообщения)

Решите линейное сравнение вида:

$$a \cdot x \equiv b \pmod m,$$

где a и m – параметры системы, а b – зашифрованное сообщение (или его фрагмент).

В ходе решения необходимо:

– определить d=НОД(a,m).

– если b не делится на d – обосновать, почему расшифрование данным методом невозможно (отсутствие решения).

– если решение существует – найти его, приведя полный расширенный алгоритм Евклида. Записать окончательный ответ в виде: $x \equiv x_0 \pmod m$ (если d=1), или $x \equiv x_0, x_1, \ldots \pmod m$ (если d>1).

Практическая работа №2

Тема: Применение китайской теоремы об остатках (решение систем сравнений, восстановление числа по модулям)

Задание 1. Прямое применение КТО (восстановление числа по остаткам)

Дана система сравнений:

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ x \equiv a_3 \pmod{m_3}, \end{cases}$$

где модули m_1, m_2, m_3 являются попарно взаимно простыми.

Необходимо:

1. Проверить условие попарной взаимной простоты модулей (найти НОД(m_i, m_j) для всех пар).
2. Вычислить общий модуль $M=m_1 \cdot m_2 \cdot m_3$.
3. Найти частичные произведения M_1, M_2, M_3.
4. С помощью расширенного алгоритма Евклида найти мультипликативные обратные элементы $y_i=M_i^{-1} \bmod m_i$.
5. Собрать решение по формуле КТО и привести ответ $x \bmod M$.

Задание 2. КТО для ускорения расшифрования в RSA (CRT-RSA)

В криптосистеме RSA известны:

– Два простых числа: p и q (соответственно, $n=p \cdot q$).

– Закрытая экспонента d.

– Шифротекст c.

Для ускорения расшифрования вместо вычисления $m=c^d \bmod n$ используют китайскую теорему об остатках, вычисляя:

$$m_1=c^d \bmod p,\ m_2=c^d \bmod q,$$

а затем восстанавливая m из системы:

$$\begin{cases} m \equiv m_1 \pmod{p}, \\ m \equiv m_2 \pmod{q}. \end{cases}$$

В данной части работы (упрощённый вариант) требуется:

Решить систему сравнений:

$$\begin{cases} x \equiv a \pmod{p}, \\ x \equiv b \pmod{q}, \end{cases}$$

где p и q – заданные взаимно простые числа (простые или просто нечётные).

Необходимо:

1. Найти $M=p \cdot q$.
2. Используя расширенный алгоритм Евклида, выразить 1 через p и q (коэффициенты Безу), либо вычислить обратные элементы $M_1^{-1} \bmod p$ и $M_2^{-1} \bmod q$.
3. Восстановить $x \bmod M$.
4. Сделать проверку подстановкой в исходную систему.

Задание 3. Криптоанализ (решение системы при немодулярных условиях)

В некоторых атаках на RSA при малой экспоненте возникает система сравнений с разными модулями. Решите систему сравнений:

$$\begin{cases} x \equiv r_1 \pmod{s_1}, \\ x \equiv r_2 \pmod{s_2}, \end{cases}$$

где модули s_1 и s_2 не обязаны быть взаимно простыми.

Необходимо:

1. Найти $d=\text{НОД}(s_1, s_2)$.
2. Проверить условие разрешимости: $r_1 \equiv r_2 \pmod{d}$.

– Если условие не выполнено – система несовместна, обосновать невозможность восстановления ключа/сообщения.

– Если условие выполнено – свести систему к эквивалентной системе с взаимно простыми модулями и решить её через КТО.

РАЗДЕЛ 2. КЛАССИЧЕСКИЕ И СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ КРИПТОАЛГОРИТМЫ

Практическая работа №3

Тема: Ручное шифрование и дешифрование шифром Цезаря и Атбаш. Частотный анализ

Задание 1. Шифр Цезаря (прямое и обратное преобразование)

1. Шифрование.

Дан открытый текст на русском языке (или английском – по варианту).

Используя шифр Цезаря с заданным ключомk*k* (сдвиг), зашифруйте текст.

2. Дешифрование (с известным ключом).

Дан криптотекст, полученный шифром Цезаря. Известен ключ *k*. Выполните дешифрование и восстановите исходное сообщение.

Задание 2. Шифр Атбаш (замена на основе обратного алфавита)

1. Шифрование.

Дан открытый текст. Зашифруйте его с использованием шифра Атбаш (подстановка: *A*↔*Z, B*↔*Y,* …).

2. Дешифрование.

Дан криптотекст, полученный шифром Атбаш. Дешифруйте его.

Указание: *В шифре Атбаш процесс шифрования и дешифрования идентичен (инволютивность). В ответе достаточно показать таблицу замен и результат.*

Задание 3. Частотный анализ (дешифрование без ключа)

Дан криптотекст средней длины (от 150 до 300 символов), полученный с помощью шифра Цезаря, но ключ неизвестен.

Необходимо:

1. Выписать криптотекст.

2. Составить частотную таблицу для всех букв криптотекста (абсолютные частоты). Для удобства отсортировать буквы по убыванию частоты.

3. Сравнить наиболее частые буквы криптотекста с эталонными частотами букв русского (или английского) языка (например, в русском: О>Е>А>И>Н>Т>С; в английском: E>T>A>O>I>N).

4. На основе частотного анализа определить предполагаемый сдвиг *k*.

5. Выполнить дешифрование с найденным сдвигом и получить осмысленный открытый текст.

6. Если полученный текст содержит ошибки, выполнить корректировку (ручной перебор соседних сдвигов или замена отдельных букв с учетом частот биграмм/триграмм – если позволяет время).

Указания к выполнению:

– Для определения сдвига найдите разницу между позицией самой частой буквы криптотекста и позицией буквы «О» (для русского) или «E» (для английского) в алфавите.

– Проверьте гипотезу на второй и третьей по частоте буквах.

– Если гипотеза не подтверждается (текст не читается), переберите вручную 2-3 соседних значения сдвига.

Варианты индивидуальных заданий

№ варианта	Задание 1. Открытый текст / Ключ *k*	Задание 2. Открытый текст	Задание 3. Криптотекст для частотного анализа
1	«криптография основа безопасности» / *k*=7	«информационная безопасность»	*(длинный текст, зашифрованный неизвестным сдвигом)*
2	«алгоритм шифрования заменой» / *k*=15	«дешифрование методом подбора»	…

Практическая работа №4

Тема: Шифрование и дешифрование шифром Виженера. Определение длины ключа

Задание 1. Шифрование и дешифрование шифром Виженера (с известным ключом)

1. Шифрование.

Дан открытый текст на русском (или английском) языке и ключевое слово K*K*.

Зашифруйте текст с использованием шифра Виженера. Покажите процесс преобразования: для каждой буквы открытого текста укажите соответствующую букву ключа (с учётом циклического повторения) и результат сложения по модулю *m*.

2. Дешифрование.

Дан криптотекст, полученный шифром Виженера, и ключевое слово *K*. Выполните дешифрование и восстановите исходное сообщение.

Задание 2. Определение длины ключа методом Касиски

Дан криптотекст средней длины (от 200 до 500 символов), полученный шифром Виженера с неизвестным ключевым словом.

Необходимо:

1. Найти в криптотексте повторяющиеся последовательности букв (подстроки) длиной 3 или 4 символа (триграммы/тетраграммы).

2. Для каждой найденной повторяющейся последовательности определить расстояние между её первыми вхождениями (в символах).

3. Вычислить наибольший общий делитель НОД всех найденных расстояний (или выбрать наиболее часто встречающееся расстояние).

4. Сделать предположение о длине ключа *L*. Если расстояния варьируются, взять наиболее вероятное значение *L*.

Указание: Метод Касиски основан на том, что повторяющиеся последовательности в криптотексте возникают, когда одинаковые фрагменты открытого текста попадают на одни и те же позиции ключа. Расстояние между ними кратно длине ключа.

Задание 3. Определение длины ключа методом Фридмана (индекс совпадений)

Дан тот же криптотекст (или новый, по варианту). Определить длину ключа *L* с использованием индекса совпадений I_c.

Необходимо:

1. Вычислить индекс совпадений для всего криптотекста $I_{общ}$:

$$I_c = \frac{\sum_{i=1}^{m} n_i(n_i - 1)}{N(N-1)},$$

где N – общая длина текста, n_i – количество вхождений i-й буквы алфавита, m – размер алфавита.

2. Сравнить полученное значение с эталонными:

– Для русского языка: $I_{случ}$≈0,030 (случайный текст), $I_{осм}$≈0,056 (осмысленный текст).

– Для английского: $I_{случ}$≈0,038, $I_{осм}$≈0,066.

3. Используя формулу Фридмана для приблизительной оценки длины ключа:

$$L \approx \frac{I_{\text{осм}} - I_{\text{случ}}}{I_{\text{общ}} - I_{\text{случ}}}.$$

(или более точная формула: L≈(027·N)/((N−1)·$I_{общ}$−0,038·N+0,0650,027) для английского).

4. Сравнить полученную оценку длины ключа с результатом метода Касиски. Сделать вывод о наиболее вероятной длине ключа L.

Указание: Если $I_{общ}$ близок к $I_{осм}$, длина ключа мала (вероятно, L=1, т.е. это шифр Цезаря). Если близок к $I_{случ}$ – длина ключа велика (возможно, равна длине текста, как в шифре Вернама, который теоретически стоек).

Варианты индивидуальных заданий

№ варианта	Задание 1. Открытый текст / Ключ K	Задание 2, 3. Криптотекст для анализа (длина от 200 символов)
1	«криптографические методы защиты информации» / K=»БЕЗОПАСНОСТЬ»	*(длинный криптотекст с неизвестным ключом)*
2	«симметричное шифрование применяется повсеместно» / K=»КЛЮЧ»	...
3	«современная криптография использует сложные алгоритмы» / K=»СТОЙКОСТЬ»	...

Практическая работа №5

Тема: Шифры перестановки: построение маршрутных таблиц

Задание 1. Прямоугольная перестановка (построчное заполнение – столбцовое считывание)

1. Шифрование.

Дан открытый текст и количество столбцов n (или ключевое слово, определяющее количество столбцов и их порядок).

Необходимо:

1. Записать открытый текст без пробелов (или с сохранением пробелов – по указанию).
2. Построить таблицу с n столбцами.
3. Заполнить таблицу по строкам (слева направо).
4. Если последняя строка заполнена не полностью, добавить символы-заполнители.
5. Считать криптотекст по столбцам (сверху вниз, слева направо) или в порядке, заданном ключом перестановки столбцов.

2. Дешифрование.

Дан криптотекст, количество столбцов n и порядок считывания столбцов.

Необходимо:

1. Записать криптотекст в столбцы таблицы в том порядке, в котором они считывались при шифровании.
2. Заполнить таблицу.
3. Считать открытый текст по строкам (слева направо).
4. Удалить символы-заполнители.

Задание 2. Маршрутное шифрование (заполнение и считывание по спирали)

1. Шифрование (спираль внутрь).

Дан открытый текст. Требуется зашифровать его, записывая текст в таблицу по спирали (по часовой стрелке, от внешнего кольца к центру), а считывать – по строкам (слева направо, сверху вниз).

Необходимо:

1. Определить размеры таблицы (количество строк и столбцов) так, чтобы они были наиболее близки к квадрату (или по указанию преподавателя).
2. Заполнить таблицу, двигаясь по спирали (→ вниз ← вверх → ...).
3. Если текст короче таблицы, оставшиеся ячейки заполнить символами-заполнителями.
4. Считать криптотекст построчно (или по столбцам – в зависимости от варианта).

2. Дешифрование.

Дан криптотекст и размеры таблицы. Требуется выполнить обратное преобразование: записать криптотекст в таблицу в порядке считывания, затем прочитать открытый текст по спирали.

Задание 3. Перестановка столбцов с ключевым словом (усложнённый вариант)

1. Шифрование.

Дан открытый текст и ключевое слово К*К* (например, "КЛЮЧ"). Количество столбцов равно длине ключевого слова. Столбцы переставляются в алфавитном порядке букв ключа (или в порядке, заданном числовым ключом).

Необходимо:

1. Записать открытый текст в таблицу по строкам.
2. Определить порядок перестановки столбцов: отсортировать буквы ключевого слова в алфавитном порядке (или использовать числовой ключ {3,1,4,2}).
3. Считать криптотекст, читая столбцы в новом порядке.
4. Записать результат шифрования.

2. Дешифрование.

Дан криптотекст и ключевое слово *К*.

Необходимо:

1. Определить порядок столбцов при шифровании.
2. Восстановить исходный порядок столбцов.
3. Записать криптотекст в столбцы таблицы в правильном порядке.
4. Считать открытый текст по строкам.

Указание: Если в таблице есть неполная последняя строка, при дешифровании необходимо учитывать, сколько символов было в последней строке, чтобы правильно распределить их по столбцам. Обычно это определяется остатком от деления длины текста на количество столбцов.

Варианты индивидуальных заданий

№ варианта	Задание 1. Открытый текст / *n* столбцов	Задание 2. Открытый текст / размер таблицы	Задание 3. Открытый текст / ключевое слово *К*
1	«перестановка изменяет порядок символов» / *n*=5	«шифрование методом спирального обхода» / 4×6	«криптографические алгоритмы перестановки» / "*К*=»БЕЗОПАСНОСТЬ»
2	«маршрутное шифрование используется в криптографии» / *n*=6	«заполнение таблицы по спирали против часовой стрелки» / 5×5	«современные шифры применяют перестановку блоков» / *К*=»СТОЙКОСТЬ»

Практическая работа №6

Тема: Анализ режимов шифрования блочных алгоритмов (ECB и CBC) – сравнение визуальных различий на примере изображений

Задание 1. Ручное шифрование изображения в режиме ECB

Дано простое монохромное изображение (например, чёрно-белый квадрат с рисунком) в виде матрицы пикселей с градациями серого (0-255) или в виде бинарной матрицы (0 – белый, 1 – чёрный). Размер изображения небольшой (например, 4×4 или 6×6 пикселей).

Необходимо:

1. Разбить изображение на блоки фиксированного размера (например, 2×2 или 1×4 байта/пикселя).
2. Для каждого блока применить упрощённую функцию шифрования (например, XOR с фиксированным ключевым байтом или перестановку значений внутри блока).
3. Записать результат в виде новой матрицы, представляющей зашифрованное изображение.
4. Визуализировать результат: схематически изобразить исходное изображение и зашифрованное (например, используя символы ▉ и ▒ для чёрного и белого, или шкалу серого).

Ожидаемый результат: При шифровании в режиме ECB структура исходного изображения сохраняется – одинаковые блоки (участки одного цвета) шифруются одинаково, поэтому на зашифрованном изображении видны контуры исходного рисунка.

Задание 2. Ручное шифрование изображения в режиме CBC

Используется то же исходное изображение, что и в Части А. Размер блока – такой же. Задан начальный вектор инициализации IV (например, случайный блок того же размера, заполненный значениями 128 или 42).

Необходимо:

1. Разбить изображение на блоки.
2. Выполнить операцию XOR первого блока открытого текста с IV.
3. Зашифровать полученный блок (использовать ту же упрощённую функцию шифрования, что и в Части А).
4. Полученный блок шифротекста использовать как IV для следующего блока (XOR со следующим блоком открытого текста, затем шифрование).
5. Повторить для всех блоков.
6. Записать результат в виде матрицы зашифрованного изображения.
7. **Визуализировать** результат.

Ожидаемый результат: При шифровании в режиме CBC структура исходного изображения полностью скрывается – даже если на изображении есть большие одноцветные области, шифротекст выглядит как случайный шум. Визуально зашифрованное изображение не содержит никаких следов исходного контура.

Задание 3. Сравнительный анализ и выводы

Используя результаты задания 1 и 2, выполнить сравнительный анализ:

Необходимо:

1. Сопоставить визуальные результаты шифрования в режимах ECB и CBC.
2. Описать, какие структурные элементы исходного изображения сохранились в каждом из режимов.
3. Объяснить, почему режим ECB не рекомендуется для шифрования данных, имеющих повторяющиеся структуры (изображения, базы данных, документы с повторяющимися заголовками).
4. Объяснить, почему режим CBC требует использования случайного или псевдослучайного IV для каждого сеанса шифрования.
5. Сформулировать вывод о том, в каких случаях допустимо использование ECB (например, для шифрования коротких уникальных сообщений, где размер блока не превышает длину данных).

Указание: При визуализации можно использовать следующие уровни серого (для 2×2 блоков):

– Вычислить среднее арифметическое значений пикселей в блоке и округлить до целого (0-255).
– Или использовать пороговое значение (например, > 128 – чёрный, ≤ 128 – белый).

Варианты индивидуальных заданий

№ варианта	Исходное изображение (матрица)	Размер блока	Ключ шифрования (XOR)	IV (для CBC)
1	6×6 матрица с буквой «Т»	2×2	0b10101010 (170)	0b11110000 (240)
2	8×8 матрица с крестом	2×2	0b11001100 (204)	0b00110011 (51)
3	4×4 матрица с квадратом в центре	1×4 (строка)	0b01010101 (85)	0b10101010 (170)

Пример исходного изображения (6×6, буква «Т»):

111111
001000
001000
001000
001000
001000

РАЗДЕЛ 3. АСИММЕТРИЧНАЯ КРИПТОГРАФИЯ

Практическая работа №7

Тема: Ручной расчёт RSA (выбор простых чисел, вычисление открытой и закрытой экспоненты, шифрование и расшифрование чисел)

Задание 1. Генерация ключевой пары RSA

Даны два простых числа p и q (или даны составные числа для проверки простоты – по указанию преподавателя).

Необходимо:

1. Вычислить модуль $n=p\cdot q$.
2. Вычислить функцию Эйлера $\varphi(n)=(p-1)\cdot(q-1)$.
3. Выбрать открытую экспоненту e (из предложенного набора или самостоятельно) такую, что:

– $1<e<\varphi(n)$

– НОД$(e, \varphi(n))=1$

– Для проверки взаимной простоты использовать алгоритм Евклида.

4. Используя расширенный алгоритм Евклида, вычислить закрытую экспоненту $d=e^{-1} \bmod \varphi(n)$.
5. Выполнить проверку: $(e\cdot d) \bmod \varphi(n)=1$.
6. Записать открытый ключ (e,n) и закрытый ключ (d,n).

Задание 2. Шифрование сообщения

Дано числовое сообщение m (или текст, преобразованный в число по таблице ASCII или другому правилу). Значение m должно удовлетворять условию: $0\le m<n$.

Необходимо:

1. Используя открытый ключ (e,n), вычислить шифротекст:

$$c = m^e \bmod n$$

2. Показать процесс возведения в степень по модулю (с использованием метода последовательного умножения или быстрого возведения в степень).
3. Записать полученное значение c.

Указание: Для ручного расчёта используйте метод "возведение в квадрат и умножение" (бинарное возведение в степень), чтобы минимизировать количество операций.

Задание 3. Расшифрование сообщения

Дан шифротекст c, полученный в задании 2, и закрытый ключ (d,n).

Необходимо:

1. Используя закрытый ключ, восстановить исходное сообщение:

$$m' = c^d \bmod n$$

2. Показать процесс возведения в степень по модулю.
3. Проверить, что $m'=m$ (расшифрование выполнено корректно).
4. Если исходное сообщение было текстовым, преобразовать числовой результат обратно в текст.

Варианты индивидуальных заданий:

№ варианта	p	q	Предлагаемые e	Сообщение m
1	47	71	3, 5, 7, 11, 17	1234
2	53	61	5, 7, 13, 17, 19	2024
3	43	79	3, 7, 11, 13, 23	5678
4	59	67	5, 11, 13, 17, 29	8888
5	41	83	3, 5, 7, 11, 31	9999
6	61	73	7, 11, 13, 17, 19	12345
7	37	97	3, 5, 11, 13, 17	5555
8	71	79	5, 7, 11, 13, 23	7777

РАЗДЕЛ 4. КРИПТОГРАФИЧЕСКИЕ ХЕШ-ФУНКЦИИ

Практическая работа №8

Тема: Криптографические хеш-функции

Задание 1. Реализация упрощённой хеш-функции (базовый алгоритм)

Дана спецификация упрощённой хеш-функции H со следующими параметрами:

– Размер блока: 8 бит (1 байт).

– Размер хеша: 8 бит (1 байт).

– Функция сжатия: $H_{нов}=(H_{стар}\oplus блок)\lll 3$ (циклический сдвиг влево на 3 бита после XOR) или другая аналогичная.

– Начальное состояние (IV): $H_0=0x00$ или $0x5A$.

Необходимо:

1. Вычислить хеш для заданного сообщения M (длиной 2-4 байта).
2. Показать пошагово:
– Разбивку сообщения на блоки.
– Применение функции сжатия к каждому блоку.
– Промежуточные состояния (после каждого блока).
– Финальное значение хеша.
3. Представить результат в двоичном и шестнадцатеричном виде.

Пример сообщения: M=1011001001101001 (2 байта)

Задание 2. Анализ лавинного эффекта

Используя ту же хеш-функцию из задания 1, выполнить анализ лавинного эффекта.

Необходимо:

1. Взять исходное сообщение M_1 (то же, что в задании 1).
2. Создать сообщение M_2, которое отличается от M_1 ровно в одном бите (например, инвертировать старший бит первого байта).
3. Вычислить хеш $H(M_2)$.
4. Сравнить $H(M)$ и $H(M_2)$ побитово:
– Подсчитать количество отличающихся бит.
– Вычислить процент отличающихся бит (отличия / размер хеша×100%).
5. Изменить другой бит (или два бита) и повторить анализ (минимум 3 различных модификации).
6. Сделать вывод о лавинном эффекте: насколько сильно меняется хеш при малом изменении входных данных.

Ожидаемый результат: Даже при изменении одного бита сообщения, хеш должен измениться примерно на 50% бит (для хорошей хеш-функции). Если изменение меньше 25%, это указывает на слабость функции.

Задание 3. Поиск коллизий (анализ устойчивости)

Используя ту же упрощённую хеш-функцию (8-битный хеш), выполнить поиск коллизий.

Необходимо:

1. Сгенерировать все возможные 8-битные сообщения (от 0x00 до 0xFF) – 256 значений.
2. Для каждого сообщения вычислить хеш (использовать функцию из Части А, без разбивки на блоки, так как сообщение равно блоку).
3. Найти хотя бы одну коллизию – два различных сообщения $M_a \neq M_b$, для которых $H(M_a)=H(M_b)$.
4. Записать найденные коллизии.
5. Оценить среднее количество сообщений, приходящихся на один хеш (по принципу Дирихле: 256 сообщений / 256 хешей = 1, но фактически из-за несовершенства функции могут быть и >1).
6. Сделать вывод о практической стойкости упрощённой хеш-функции к коллизиям.

Указание: Поскольку хеш 8-битный, коллизии гарантированно существуют (принцип Дирихле). Задача – найти их вручную и убедиться в возможности подбора.

Задание 4. Контроль целостности и хеширование с солью

1. Контроль целостности.

Даны два файла (представлены в виде битовых строк):

– Файл A: «Hello, World!»
– Файл B: «Hello, World?» (отличается одним символом, но предположительно злоумышленник утверждает, что файлы идентичны).

Необходимо:

1. Вычислить хеш для каждого файла (использовать ту же упрощённую функцию, разбивая на блоки по 8 бит).
2. Сравнить хеши и сделать вывод о целостности.

2. Хеширование паролей с солью.

Дан пароль пользователя P="*pass*123". Требуется сохранить его в базе данных в виде хеша с солью.

Необходимо:

1. Сгенерировать случайную соль S (например, 4 бита или 8 бит).
2. Вычислить хеш от конкатенации ($S||P$).
3. Записать результат в виде: хранится=(S,$H(S||P)$).
4. Показать, что даже если два пользователя имеют одинаковый пароль, их хеши в базе данных будут различаться (из-за разных солей).

Варианты индивидуальных заданий

№ варианта	Начальный IV H_0	Функция сжатия	Сообщение M (битовая строка)	Соль S (для Г2)
1	0x00	$H=(H \oplus block) \lll 3$	10110010 01101001 11000101	1010
2	0x5A	$H=(H \oplus block) \lll 2$	01101001 11000101 10110010	1100
3	0xFF	$H=(H \oplus block) \lll 4$	11000101 10110010 01101001	1001
4	0x3C	$H=(H \oplus block) \ggg 2$	00101101 10011100 01011010	0110
5	0xA5	$H=(H \oplus block) \lll 5$	11100010 01011010 10110101	1110

Примечание: $\lll k$ – циклический сдвиг влево на k бит; $\ggg k$ – циклический сдвиг вправо наkk бит.

РАЗДЕЛ 5. ЭЛЕКТРОННАЯ ПОДПИСЬ И ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ

Практическая работа №9

Тема: Работа с сертифицированным СКЗИ для ЭП (генерация ключей, подписание документа, проверка)

Задания:

Задание 1. Генерация ключевой пары ЭП

Моделирование процесса создания закрытого и открытого ключей с использованием заданных параметров и алгоритма на основе ГОСТ Р 34.10-2012.

Исходные данные: Параметр кривой (задан номером варианта), закрытый ключ d (в виде числа), базовая точка P эллиптической кривой, параметры кривой a и b, порядок группы q.

Необходимо:

1. С использованием заданного закрытого ключа d вычислить открытый ключ $Q=d \cdot P$ (умножение точки эллиптической кривой на скаляр, с демонстрацией операций сложения и удвоения точек).
2. Смоделировать формирование запроса на сертификат: сгенерировать структуру, содержащую открытый ключ Q, идентификационные данные пользователя (условно) и подпись запроса закрытым ключом (реализовать расчёт хеша и подпись по ГОСТ Р 34.10-2012).
3. Зафиксировать результат в виде отчёта: значения параметров, вычисленный открытый ключ, хеш запроса.

Задание 2. Подписание документа

Моделирование процесса создания отсоединённой электронной подписи под документом.

Исходные данные: Текстовый документ M (задан строками). Закрытый ключ d и параметры кривой из Части А. Сертификат ключа проверки ЭП (условный, с заданными полями).

Необходимо:

1. Вычислить хеш-значение документа $h=H(M)$ с использованием хеш-функции по ГОСТ Р 34.11-2012 (Стрибог) – выполняется расчёт по упрощённой схеме или с использованием таблиц замен, аналогично Практической работе №8.
2. Сгенерировать случайное число k (задано в варианте) и вычислить точку эллиптической кривой $C=k \cdot P$.
3. Вычислить число $r=x_C \bmod q$, где x_C – координата x точки C. Если $r=0$, повторить с новым k.
4. Вычислить число $s=(k^{-1} \cdot (h+d \cdot r)) \bmod q$. Если $s=0$, повторить с новым k.
5. Сформировать ЭП как пару чисел (r,s) в формате, соответствующем ГОСТ Р 34.10-2012.
6. Создать файл подписи с расширением .sig, добавив к нему метаданные (например, время подписания).

Задание 3. Проверка электронной подписи

Моделирование процесса проверки корректности подписи под документом.

Исходные данные: Исходный документ M (из Части Б). Файл подписи (r,s). Открытый ключ Q и сертификат (из Части А). Параметры кривой.

Необходимо:

1. Вычислить хеш документа $h'=H(M)$ заново (должен совпасть с h, если документ не изменён).
2. Проверить условия: $0<r<q$ и $0<s<q$.
3. Вычислить: $w=s^{-1} \bmod q$, $u_1=(h'\cdot w) \bmod q$, $u_2=(r\cdot w) \bmod q$.
4. Вычислить точку: $C'=u_1\cdot P+u_2\cdot Q$ (операции сложения и удвоения точек на эллиптической кривой).
5. Вычислить $r'=x_{C'} \bmod q$. Если $r'=r$, подпись корректна. В противном случае – подпись недействительна.
6. Смоделировать ситуацию с изменённым документом (инвертировать один бит в тексте) и повторить проверку, убедившись в отрицательном результате.
7. Зафиксировать результат проверки (например, «Подпись проверена» или «Подпись не верна»).

Задание 4. Анализ структуры ЭП и сертификата

Необходимо:

1. Проанализировать формат электронной подписи в формате CAdES-BES: определить, какие данные входят в состав подписи (подписанные данные, сертификаты, информация об алгоритмах).
2. Смоделировать проверку сертификата: проверить его срок действия (задан в варианте), цепочку сертификации, подпись УЦ.
3. Объяснить, какие действия предпринимаются при проверке подписи с меткой доверенного времени (CAdES-T).

Практическая работа №10

Тема: Анализ протоколов аутентификации (сравнение парольных, токенных и криптографических протоколов)

Задание 1. Анализ парольного протокола аутентификации

Рассматривается классическая схема аутентификации по паролю в клиент-серверной архитектуре.

Сценарий: Пользователь вводит логин и пароль на веб-странице. Сервер проверяет введённые данные, сравнивая хеш пароля с сохранённым в базе данных (с солью).

Необходимо:

1. Описать полную последовательность действий при аутентификации (от ввода пароля до получения доступа).
2. Выделить уязвимые места протокола:

– Передача пароля по сети (если нет TLS).
– Хранение хешей паролей в БД (риск компрометации).
– Атака перебором (bruteforce) – онлайн и офлайн.
– Фишинг (поддельная страница ввода пароля).
– Повторная передача (replay attack), если нет защиты.

3. Предложить меры защиты для каждой уязвимости.
4. Сделать вывод об области применения парольной аутентификации и её ограничениях.

Варианты для анализа:

– HTTP Basic Authentication (передача в открытом виде).
– Аутентификация с хешированием пароля на клиенте (CHAP).
– Kerberos (парольная фаза с использованием KDC).

Задание 2. Анализ токенного протокола аутентификации

Рассматривается схема аутентификации с использованием одноразовых паролей (OTP) на основе времени (TOTP) согласно RFC 6238.

Сценарий: Пользователь вводит логин и пароль (первый фактор). Затем вводит 6-значный код из приложения-аутентификатора (Google Authenticator, АО «МТС» и др.), который меняется каждые 30 секунд.

Необходимо:

1. Описать алгоритм генерации TOTP на основе секретного ключа K и текущего времени T:

$$TOTP(K,T)=Truncate(HMAC\text{-}SHA1(K,T)) \bmod 10^6$$

2. Описать, как сервер проверяет введённый код (вычисляет своё значение и сравнивает с учётом допустимого временного окна).

3. Провести анализ уязвимостей протокола:

– Утечка секретного ключа K (при первоначальной передаче или из скомпрометированного устройства).

– Фишинг с перехватом OTP (последующее использование ограничено 30 секундами, но атака «человек посередине» (MITM) может передать код в реальном времени).

– Синхронизация времени (если время на устройстве рассинхронизировано).

– Социальная инженерия (запрос OTP у пользователя).

4. Сравнить TOTP с HOTP (на основе счётчика) – в чём преимущества и недостатки.

5. Сделать вывод о стойкости токенной аутентификации по сравнению с парольной.

Задание 3. Анализ криптографического протокола аутентификации

Рассматривается протокол аутентификации на основе сертификатов (асимметричная криптография), например, в рамках TLS с взаимной аутентификацией.

Сценарий: Пользователь (клиент) и сервер обмениваются сертификатами, подписанными доверенным удостоверяющим центром. Аутентификация выполняется с помощью проверки электронной подписи и доказательства владения закрытым ключом.

Необходимо:

1. Описать последовательность шагов протокола TLS с двусторонней аутентификацией (mTLS):

– Установление TLS-соединения.

– Обмен сертификатами.

– Проверка сертификатов клиентом и сервером (проверка подписи УЦ, срока действия, списка отозванных сертификатов).

– Генерация и обмен ключевыми материалами (алгоритм Диффи-Хеллмана или RSA).

– Доказательство владения закрытым ключом (подпись определённых данных).

2. Провести анализ устойчивости протокола к следующим атакам:

– Перехват и подмена трафика (MITM) – защищён асимметричным шифрованием и сертификатами.

– Повторная атака – защищена использованием случайных nonce и временных меток.

– Компрометация закрытого ключа – требуется немедленный отзыв сертификата.

– Атака на сертификационный центр (компрометация УЦ) – возможна, но требует сложных действий.

3. Сравнить криптографическую аутентификацию с парольной и токенной по критериям:

– Стойкость.

– Сложность внедрения.

– Пользовательский опыт (использование смарт-карт, токенов PKCS#11).

– Стоимость владения.

4. Рассмотреть альтернативные криптографические протоколы:

– Протокол Шнорра (аутентификация с нулевым разглашением).

– Протокол Диффи-Хеллмана с аутентификацией (STS – Station-to-Station).

Задание 4. Сравнительный анализ и выбор протокола

На основе анализа трёх типов протоколов выполнить их сравнение по следующей таблице:

Критерий	Парольный	Токенный (OTP)	Криптографический (сертификаты)
Стойкость к перебору	Низкая (зависит от пароля)	Высокая (случайный 6-значный код)	Очень высокая (длина ключа ≥ 1024 бит)
Стойкость к сниффингу	Низкая (если без TLS)	Высокая (код одноразовый)	Высокая (закрытый ключ не передаётся)
Стойкость к повтору (replay)	Низкая	Высокая (код одноразовый)	Высокая (nonce, метки времени)
Стойкость к MITM	Низкая	Средняя (без дополнительной защиты)	Высокая (сертификаты)
Стойкость к фишингу	Низкая	Средняя (код одноразовый)	Высокая (невозможно подделать подпись)
Удобство для пользователя	Высокое (ввод пароля)	Среднее (ввод пароля + кода)	Низкое (требуется токен/смарт-карта)
Сложность внедрения	Низкая	Средняя	Высокая (требуется PKI)

Стоимость владения	Низкая	Средняя	Высокая

Необходимо:

1. Заполнить таблицу для трёх протоколов (включая обоснование каждого балла).
2. Выбрать наиболее подходящий протокол для следующих сценариев (с обоснованием):

– Сценарий 1: Интернет-банкинг (высокие требования к безопасности, пользователи – физические лица).

– Сценарий 2: Внутренняя корпоративная система (сотрудники, доступ с рабочих станций в защищённой сети).

– Сценарий 3: Мобильное приложение для оплаты (необходим высокий уровень удобства и защиты).

– Сценарий 4: Доступ к государственным информационным системам (строгие регуляторные требования).

Варианты индивидуальных заданий

№ варианта	Парольный протокол для анализа	Токенный протокол для анализа	Криптографический протокол для анализа	Сценарий для выбора протокола
1	HTTP Basic Auth	TOTP	mTLS (взаимная)	Интернет-банкинг
2	CHAP	HOTP	Kerberos	Корпоративная почта
3	PAP (PPP)	RSA SecurID	TLS с сертификатами	Мобильное приложение
4	NTLM (Windows)	FIDO U2F	STS протокол	Государственная ЭП

РАЗДЕЛ 6. ПРИКЛАДНЫЕ АСПЕКТЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Практическая работа №11

Тема: Настройка защищённого соединения SSL/TLS (веб-сервер, анализ сертификатов, проверка шифров)

Задание 1. Генерация ключей и самоподписанного сертификата

В реальных условиях сертификат подписывается Удостоверяющим центром (CA). В данной работе для тестирования используется самоподписанный сертификат.

Необходимо:

1. Установить пакет openssl, если он не установлен в системе.
2. Сгенерировать закрытый ключ (приватный ключ) длиной 2048 бит:

openssl genrsa -out server.key 2048

Важно: закрытый ключ должен иметь права доступа 600 (chmod 600 server.key).

3. Создать запрос на сертификат (CSR). В процессе заполнить информацию об организации (Common Name должен совпадать с доменным именем сервера):

openssl req -new -key server.key -out server.csr

4. Сгенерировать самоподписанный сертификат X.509 сроком на 365 дней:

openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

5. Зафиксировать в отчёте содержимое сертификата для его анализа:

openssl x509 -in server.crt -text -noout

Результат: в отчёте должны быть отражены серийный номер, алгоритм подписи, срок действия и информация о владельце (Subject).

Задание 2. Настройка веб-сервера для работы с HTTPS

Настройка выполняется для веб-сервера NGINX (по выбору студента или указанию преподавателя может быть Apache).

Необходимо:

1. Убедиться, что модуль SSL загружен, и конфигурация сервера синтаксически корректна:

nginx -V 2>&1 | grep with-http_ssl_module

nginx -t

2. Создать конфигурацию виртуального хоста для порта 443:

nginx

server {

listen 443 ssl;

```
    server_name your_domain.com; # Заменить на CN из сертификата

    ssl_certificate /path/to/server.crt;
    ssl_certificate_key /path/to/server.key;
    # Базовая конфигурация для безопасности
    ssl_protocols TLSv1.2 TLSv1.3; # Отключение устаревших SSL/TLS [citation:5][citation:10]
    ssl_prefer_server_ciphers on;
    location / {
        root /var/www/html;
        index index.html;
    }
}
```

3. Перезагрузить конфигурацию веб-сервера:

systemctl reload nginx

4. Убедиться, что порт 443 открыт в брандмауэре:

ufw allow 443/tcp

Задание 3. Анализ сертификатов и проверка шифров

Анализ выполняется с использованием команд OpenSSL и онлайн-инструментов.

Необходимо:

1. Анализ установленного сертификата:

– Проверить соответствие закрытого ключа и сертификата (сравнить хеш-суммы модулей):

openssl x509 -in server.crt -pubkey -noout -outform pem | openssl md5

openssl rsa -in server.key -pubout -outform pem | openssl md5

– Проверить цепочку сертификатов (валидация) -1:

openssl verify -CAfile server.crt server.crt

Ожидаемый результат: для самоподписанного сертификата будет ошибка, но для тестовой работы это допустимо.

2. Ручная проверка TLS-соединения:

– Выполнить рукопожатие с сервером и посмотреть на выбранный протокол и шифр:

openssl s_client -connect localhost:443 -servername your_domain.com

– В выводе команды найти строки Protocol и Cipher. Зафиксировать их в отчёте.

3. Сканирование уязвимостей:

– Использовать онлайн-сервис SSL Labs (ssllabs.com).

– Ввести IP-адрес или домен сервера и проанализировать полученный отчёт. Обратить внимание на:

– Общую оценку (A+ – отлично).

– Поддерживаемые протоколы (наличие TLS 1.0/1.1 считается уязвимостью).

– Список шифров (наличие RC4, 3DES, NULL – критично).

Варианты индивидуальных заданий

№ варианта	Веб-сервер	Домен (CN)	Дополнительное задание
1	NGINX	site1.local	Настроить HSTS
2	Apache	site2.local	Добавить параметры DH
3	NGINX	site3.local	Настроить OCSP Stapling
4	Apache	site4.local	Настроить клиентскую аутентификацию

Практическая работа №12

Тема: Разработка проекта аттестационной документации (составление перечня проверяемых требований, актов проверки)

Задание 1. Разработка перечня проверяемых требований

На основе заданного объекта информатизации (ОИ) сформировать перечень проверяемых требований в соответствии с классом защищённости объекта.

Исходные данные (по варианту):

– Тип объекта: государственная информационная система / автоматизированная система управления производственным процессом / информационная система персональных данных.

– Класс защищённости: К1, К2, К3 (по ФСТЭК) или УЗ-1, УЗ-2, УЗ-3 (по 152-ФЗ).

– Обрабатываемая информация: конфиденциальная, служебная, персональные данные.

– Состав СЗИ: сертифицированные СКЗИ (например, КриптоПро CSP), антивирус, система обнаружения вторжений, межсетевой экран.

Необходимо:

1. Изучить заданный класс защищённости и определить перечень обязательных требований:

– Организационные меры:

▪ Наличие организационно-распорядительной документации (приказы, инструкции, политики).

▪ Назначение должностных лиц, ответственных за защиту информации.

▪ Организация допуска и режима работы.

▪ Обучение сотрудников мерам безопасности.

– Инженерно-технические меры:

▪ Физическая защита объекта (пропускной режим, охрана).

▪ Защита от несанкционированного доступа (НСД) к помещениям и оборудованию.

▪ Резервирование систем электропитания и охлаждения.

– Программно-аппаратные меры:

▪ Использование сертифицированных средств защиты (СКЗИ, СОВ, МЭ, антивирус).

▪ Реализация идентификации и аутентификации.

▪ Разграничение доступа (мандатное/дискреционное).

▪ Шифрование данных (в покое и при передаче).

▪ Регистрация и учёт событий безопасности.

▪ Защита от вредоносного кода.

▪ Защита от утечек по техническим каналам (ПЭМИН, акустика).

– Меры по обеспечению целостности:

▪ Контроль целостности ПО и данных.

▪ Использование электронной подписи.

▪ Антивирусная защита.

– Меры по управлению доступом:

▪ Идентификация и аутентификация пользователей.

▪ Разграничение прав доступа к ресурсам.

▪ Контроль привилегированных учётных записей.

2. Сформировать Перечень проверяемых требований в виде таблицы:

№ п/п	Раздел/Категория требований	Конкретное требование (формулировка из НД)	Метод проверки (документальный, инструментальный, организационный)	Примечание
1.1	Организационные меры	Наличие приказа о назначении ответственного за СЗИ	Документальный	Проверить наличие приказа
1.2	Организационные меры	Наличие инструкции пользователя по работе с СЗИ	Документальный	Проверить актуальность
2.1	Идентификация и аутентификация	Парольная политика (длина, сложность, срок действия)	Инструментальный	Проверить настройки ОС/СЗИ

3. Для каждого требования указать метод проверки:

– Документальный – анализ предоставленных документов.

– Инструментальный – проведение тестов с использованием ПО/оборудования.

– Организационный – опрос персонала, визуальный осмотр.

4. Указать ссылку на нормативный документ (пункт, подпункт), обосновывающий необходимость проверки.

Результат: Готовый Перечень проверяемых требований для заданного объекта.

Задание 2. Разработка Акта проверки состояния защищённости

На основе разработанного Перечня проверяемых требований (Часть А) составить Акт проверки состояния защищённости объекта информатизации.

Необходимо:

1. Оформить Акт проверки состояния защищённости объекта информатизации по установленной форме (Приказ ФСТЭК № 31, Приложение 3). Акт должен включать:

– Шапку документа: наименование организации, дата, место составления, состав комиссии (председатель, члены комиссии, представители проверяемой организации).

– Основание для проведения проверки: план проверок, приказ руководителя, задание на проверку.

– Цель проверки: подтверждение соответствия СЗИ установленным требованиям.

– Объект проверки: наименование, назначение, класс защищённости, обрабатываемая информация.

– Результаты проверки: в виде таблицы с графами:

- № п/п.
- Проверяемое требование (ссылка на пункт НД).
- Фактический результат проверки (выполнено/не выполнено/частично выполнено).
- Выявленные недостатки (уязвимости).
- Рекомендации по устранению недостатков.
- Отметка об устранении (заполняется при повторной проверке).

– Заключение комиссии: о соответствии (несоответствии) объекта установленным требованиям с указанием уровня (класса) защищённости.

– Подписи членов комиссии.

2. Заполнить акт результатами воображаемой проверки:

– Часть требований должна быть выполнена (пометить «Выполнено»).

– Часть требований должна иметь выявленные недостатки (например, «Не выполнено: отсутствует журнал учёта событий безопасности», «Частично выполнено: парольная политика не соответствует требованиям по длине»).

– Для каждого недостатка сформулировать рекомендацию по устранению.

3. Сформулировать заключение комиссии:

– Если все требования выполнены – «Объект соответствует установленным требованиям, рекомендуется к выдаче аттестата соответствия».

– Если есть недостатки – «Объект не соответствует установленным требованиям. Необходимо устранить выявленные недостатки в установленный срок».

Результат: Готовый Акт проверки состояния защищённости объекта.

Задание 3. Разработка программы и методики проверки (ПМП)

Для аттестации объекта необходимо разработать программу и методику проверки, которая регламентирует порядок выполнения инструментального контроля.

Необходимо:

1. Разработать Программу и методику проверки (ПМП) защиты информации на объекте. Включить следующие разделы:

- Раздел 1. Общие положения:
  - Назначение документа.
  - Объект проверки.
  - Перечень нормативных документов.
- Раздел 2. Требования к средствам проверки:
  - Перечень аппаратных и программных средств, используемых при проверке (например, сканер безопасности XSpider, анализатор трафика Wireshark, OpenSSL для проверки TLS).
  - Требования к метрологическому обеспечению.
- Раздел 3. Методика проверки:
  - Пошаговое описание процедур для каждого проверяемого требования из Перечня (Часть А).
  - Ожидаемые результаты и критерии оценки.
- Раздел 4. Оформление результатов:
  - Формы протоколов инструментального контроля.
  - Порядок составления Акта проверки.

2. Для криптографических проверок описать методики:

- Проверка корректности установки и функционирования СКЗИ.
- Проверка соответствия используемых криптоалгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11.
- Проверка защищённости ключевой информации.
- Проверка работоспособности ЭП (генерация, подписание, проверка).

3. Заполнить протокол инструментальной проверки для одного из требований (например, проверка TLS-соединения с использованием OpenSSL) в виде таблицы:

Эта	Описание	Ожидаемый результат	Фактический результат	Отметка о

п	действия			выполнени и
1	Установить соединение с сервером через openssl s_client	Установка TLS-соединения	Установлено	+
2	Проверить поддерживаемы е протоколы	TLSv1.2 и TLSv1.3	TLSv1.2, TLSv1.3	+
3	Проверить используемые шифры	ECDHE-RSA-AES256-GCM-SHA38 4	ECDHE-RSA-AES256-GCM-SHA38 4	+

Результат: Раздел ПМП с методикой инструментальной проверки и заполненный протокол проверки.

Варианты индивидуальных заданий

№ варианта	Тип объекта	Класс защищённости	Обрабатываемая информация	Состав СЗИ
1	ГИС	К1 (по ФСТЭК)	Государственная тайна (совершенно секретно)	СКЗИ «КриптоПро CSP 5.0», МЭ «Континент», СОВ "Контур"
2	ИСПДн	УЗ-2 (по 152-ФЗ)	Персональные данные (спецкатегории)	СКЗИ «VipNet CSP», Антивирус Касперского, IDS
3	АСУ ТП	К2 (по ФСТЭК)	Служебная информация ограниченного доступа	СКЗИ «Signal-COM», МЭ, Антивирус, средство криптографической защиты каналов
4	ИСПДн	УЗ-3 (по 152-ФЗ)	Персональные данные (общедоступные)	СКЗИ «КриптоПро CSP 4.0», Антивирус, backup
5	ГИС	К3 (по ФСТЭК)	Открытая общедоступная информация (с элементами ЭП)	СКЗИ для ЭП, TLS

ЗАДАНИЯ НА ЛАБОРАТОРНЫЕ РАБОТЫ

РАЗДЕЛ 2. КЛАССИЧЕСКИЕ И СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ КРИПТОАЛГОРИТМЫ

Лабораторная работа №1

Тема: Программная реализация шифров простой замены (Цезарь, Атбаш) с обработкой текстовых файлов

Задание 1. Реализация шифра Цезаря

Разработать программный модуль (функцию/класс) для шифрования и дешифрования текста шифром Цезаря.

Необходимо:

1. Реализовать функции:
- caesar_encrypt(text, shift, alphabet) – шифрование текста с заданным сдвигом.
- caesar_decrypt(text, shift, alphabet) – дешифрование текста с заданным сдвигом.
2. Учесть особенности:
- Сдвиг k должен быть целым числом. Допускаются отрицательные значения (сдвиг влево).
- Если k превышает размер алфавита, использовать операцию взятия по модулю: $k_{эфф}=k \bmod m$.
- Сохранение регистра: "А" → "Б" (при сдвиге 1), "а" → "б".
- Сохранение небуквенных символов (пробелы, знаки препинания, цифры) без изменений.
3. Добавить поддержку двух алфавитов:
- Русский алфавит (32 буквы, без "Ё").
- Английский алфавит (26 букв).
- Возможность выбора алфавита через параметр функции.
4. Провести тестирование:
- Зашифровать тестовую фразу с известным ключом.
- Расшифровать полученный шифротекст и убедиться в совпадении с исходным текстом.
- Проверить работу с отрицательным сдвигом.

Пример тестового набора:

Входной текст: "Привет, Мир!"

Сдвиг (k): 3

Ожидаемый результат: "Уулкзх, Плу!"

Задание 2. Реализация шифра Атбаш

Разработать программный модуль для шифрования и дешифрования текста шифром Атбаш.

Необходимо:

1. Реализовать функцию:
- atbash(text, alphabet) – шифрование/дешифрование текста шифром Атбаш (одна функция для обоих действий).
2. Учесть особенности:
- Инволютивность шифра: atbash(atbash(text)) = text.
- Построение словаря замены: для каждой буквы алфавита i найти зеркальную букву $m-1-i$.
- Сохранение регистра.
- Сохранение небуквенных символов.
3. Поддержка алфавитов:
- Русский и английский алфавиты.
- Раздельная обработка прописных и строчных букв (чтобы "А" ↔ "Я", "а" ↔ "я").
4. Провести тестирование:
- Зашифровать тестовую фразу.
- Применить шифр повторно и убедиться в восстановлении исходного текста.

Пример тестового набора:

Входной текст: "А роза упала на лапу Азора"

Ожидаемый результат: "Я илз япздп мз лзпл Яилз"

Задание 3. Обработка текстовых файлов

Реализовать программу, которая читает текст из файла, выполняет шифрование/дешифрование и записывает результат в другой файл.

Необходимо:

1. Реализовать функции работы с файлами:
- read_file(filename) – чтение текстового файла в строку (с обработкой кодировки UTF-8).

– write_file(filename, content) – запись строки в текстовый файл.

2. Реализовать интерфейс командной строки:

python cipher.py --mode <encrypt/decrypt> --cipher <caesar/atbash> --key <shift> --input <input.txt> --output <output.txt>

или интерактивный режим с запросом параметров у пользователя.

3. Обработка ошибок:

– Если входной файл не найден – вывести сообщение об ошибке и завершить работу.

– Если ключ для шифра Цезаря не указан – запросить или использовать значение по умолчанию (например, 3).

– Если выходной файл уже существует – запросить подтверждение на перезапись.

4. Поддержка больших файлов:

– Реализовать построчное чтение и запись для экономии памяти (при работе с большими файлами).

5. Провести тестирование на реальных файлах:

– Создать текстовый файл объёмом 5-10 килобайт (например, отрывок из книги).

– Зашифровать файл шифром Цезаря.

– Зашифровать тот же файл шифром Атбаш.

– Расшифровать полученные файлы и сравнить с оригиналом (проверить целостность).

Лабораторная работа №2

Тема: Программная реализация шифра Виженера и частотного криптоанализа (автоматическое определение ключа)

Задание 1. Реализация шифра Виженера

Разработать программный модуль для шифрования и дешифрования текста шифром Виженера.

Необходимо:

1. Реализовать функции:

– `vigenere_encrypt(text, key, alphabet)` – шифрование текста с заданным ключевым словом.

– `vigenere_decrypt(text, key, alphabet)` – дешифрование текста с заданным ключевым словом.

2. Учесть особенности:

– Поддержка русского и английского алфавитов (по выбору).

– Сохранение регистра букв.

– Сохранение небуквенных символов (пробелы, знаки препинания, цифры) – они не шифруются, но учитываются при продвижении по ключу? *(Уточнить: обычно небуквенные символы пропускаются, ключ не сдвигается)*.

– Ключевое слово может быть любой длины (в том числе длиннее текста).

– Ключ приводится к нижнему регистру для единообразия.

3. Реализовать вспомогательные функции:

– `normalize_text(text)` – удаление небуквенных символов для анализа.

– `text_to_numbers(text, alphabet)` – преобразование текста в числовой вектор.

– `numbers_to_text(numbers, alphabet)` – обратное преобразование.

4. Провести тестирование:

– Зашифровать тестовую фразу с известным ключом.

– Расшифровать полученный шифротекст и убедиться в совпадении с исходным текстом.

– Проверить работу с ключом, содержащим повторяющиеся буквы.

Пример тестового набора:

Входной текст: "Шифр Виженера является полиалфавитным"

Ключ: "КЛЮЧ"

Ожидаемый результат: (рассчитывается вручную или с помощью известного онлайн-инструмента)

Задание 2. Определение длины ключа

Реализовать автоматическое определение длины ключа шифра Виженера двумя методами.

Необходимо:

1. Реализовать метод Касиски:

– `find_repeated_sequences(text, min_length=3)` – поиск всех повторяющихся последовательностей длиной не менее `min_length`.

– Для каждой последовательности найти расстояния между первыми вхождениями.
– Вычислить НОД всех расстояний (или выбрать наиболее часто встречающееся расстояние как предполагаемую длину ключа).
– Вернуть список предполагаемых длин с оценкой вероятности.
2. Реализовать метод Фридмана (индекс совпадений):
– `calculate_index_of_coincidence(text, alphabet)` –вычисление индекса совпадений для текста.

$$I_c = \frac{\sum_{i=1}^{m} n_i(n_i - 1)}{N(N-1)}$$

где n_i – количество вхождений i-й буквы, N – общая длина текста.
– `estimate_key_length(text, alphabet)` – оценка длины ключа по формуле Фридмана.
– Вернуть предполагаемую длину ключа.
3. Реализовать автоматический выбор лучшей длины ключа:
– Проанализировать несколько предполагаемых длин (например, от 2 до 20).
– Для каждой длины L разделить текст на L столбцов и вычислить средний индекс совпадений по столбцам.
– Выбрать L, при котором средний индекс совпадений максимален (близок к $I_{осм}$).
4. Провести тестирование:
– Сгенерировать шифротексты с разными длинами ключа (3, 5, 10, 15).
– Для каждого шифротекста определить длину ключа автоматически.
– Сравнить результаты с истинной длиной ключа.
– Оценить точность методов в зависимости от длины текста (100, 500, 1000, 5000 символов).
Пример вывода:
Метод Касиски:
Повторяющиеся последовательности:
"ст": расстояния 12, 24, 36 -> НОД = 12
"ро": расстояния 18, 30, 42 -> НОД = 6
Предполагаемая длина ключа: 6
Метод Фридмана:
Индекс совпадений: 0.042
Оценка длины ключа: 6.2
Выбранная длина ключа: 6

Лабораторная работа №3

Тема: Реализация генератора ПСЧ и режима гаммирования (шифрование/дешифрование файлов)
Задание 1. Реализация генератора ПСЧ
Реализовать программно один из генераторов ПСЧ (по выбору студента или по указанию преподавателя).
Варианты:
1. LFSR на 16 бит с полиномом обратной связи $x^{16}+x^5+x^3+x^2+1$.
2. FCSR на 8 разрядов с параметрами q=256.
3. BBS (Blum-Blum-Shub) на основе модуля n=p·q, где p, q – простые числа ≡3 mod 4.
4. AES-CTR – использование AES в режиме счётчика для генерации гаммы.
5. LCG (линейный конгруэнтный генератор) с параметрами a, c, m (для учебных целей, но с указанием на его нестойкость).

Необходимо:
1. Реализовать класс/функцию генератора:
– `init(seed)` – инициализация начального состояния.
– `next_byte()` – генерация следующего байта гаммы.
– `generate(length)` – генерация последовательности байт заданной длины.
2. Проверить статистические свойства:
– Сгенерировать 256 байт и проверить распределение (частоты должны быть близки).
– Проверить период генератора (для LFSR – максимальный период 2^n-1).

– Проверить корреляционные свойства (соседние байты не должны коррелировать).

3. Документировать параметры генератора:

– Полином обратной связи.

– Начальное состояние.

– Период (теоретический и фактический).

4. Реализовать тесты для разных seed:

– Убедиться, что разные seed дают разные последовательности.

– Убедиться, что одинаковые seed дают одинаковые последовательности.

Задание 2. Реализация режима гаммирования

Реализовать шифрование и дешифрование файлов в режиме гаммирования с использованием разработанного генератора ПСЧ.

Необходимо:

1. Реализовать функции:

– `encrypt_file(input_file, output_file, seed, generator_type)` – шифрование файла.

– `decrypt_file(input_file, output_file, seed, generator_type)` – дешифрование файла (идентично шифрованию, так как XOR симметричен).

2. Учесть особенности:

– Чтение и запись файлов по блокам (например, по 1024 байта) для экономии памяти.

– Генерация гаммы той же длины, что и файл.

– Поддержка любых типов файлов (текстовые, бинарные, изображения).

– XOR выполняется побайтово.

3. Реализовать сохранение seed/IV в заголовке файла:

– Чтобы расшифровать файл, нужен тот же seed.

– Для реальной безопасности seed/IV должен быть уникальным для каждого файла.

– В учебных целях можно сохранять seed в начале файла (но это нарушает безопасность).

4. Провести тестирование:

– Зашифровать текстовый файл (например, из лабораторной работы №1).

– Расшифровать полученный файл и убедиться в совпадении с оригиналом.

– Проверить работу с бинарными файлами (например, изображение или исполняемый файл).

– Проверить, что изменение одного байта в файле приводит к изменению только одного байта шифротекста (свойство поточного шифра).

5. Реализовать интерфейс командной строки:

Задание 3. Атака на основе повторного использования гаммы

Реализовать демонстрацию уязвимости режима гаммирования при повторном использовании одной и той же гаммы (seed/IV) для двух разных сообщений.

Необходимо:

1. Создать два открытых текста (например, два текстовых файла с известным содержимым).

2. Зашифровать оба текста с использованием одного и того же seed:

– $C_1=P_1 \oplus G$

– $C_2=P_2 \oplus G$

3. Вычислить XOR шифротекстов:

– $C_1 \oplus C_2=(P_1 \oplus G) \oplus (P_2 \oplus G)=P_1 \oplus P_2$

4. Восстановить открытые тексты:

– Если один из текстов известен (например, P_1 известен), то:

$$P_2=C_1 \oplus C_2 \oplus P_1$$

– Если ни один текст не известен, можно использовать статистические методы (частотный анализ) для восстановления обоих текстов.

5. Реализовать автоматическое восстановление:

– Функция `recover_plaintexts(cipher1, cipher2, known_plaintext=None)`.

– Если `known_plaintext` задан, восстановить второй текст.

– Если не задан, использовать частотный анализ для восстановления обоих текстов (с учётом пробелов).

6. Провести демонстрацию:

– Показать, что даже без знания ключа можно восстановить содержимое файлов.

– Создать отчёт с примерами восстановленных текстов.

Задание 4. Исследование свойств генераторов ПСЧ

Провести сравнительный анализ различных генераторов ПСЧ с точки зрения криптографической стойкости.

Необходимо:

1. Реализовать несколько генераторов:
   - LFSR (16 и 32 бита).
   - BBS (с разными размерами модуля).
   - AES-CTR (используя библиотечную реализацию AES).
   - LCG (для демонстрации нестойкости).
2. Провести тесты на статистическую случайность:
   - Частотный тест: проверить распределение байтов (0-255) – должно быть близко к равномерному.
   - Тест на корреляцию: проверить, что соседние байты не коррелируют (коэффициент корреляции близок к 0).
   - Тест на повторяемость: проверить период генератора (для LFSR -2^n-1).
   - Тест на энтропию: вычислить энтропию Шеннона для сгенерированной последовательности.
3. Провести тесты на криптографическую стойкость:
   - Тест на предсказуемость: восстановить состояние LFSR по известным 2n битам (алгоритм Берлекэмпа-Месси).
   - Тест на зависимость от seed: проверить, что изменение seed на 1 приводит к кардинальному изменению гаммы (лавинный эффект).
4. Сравнить производительность:
   - Измерить скорость генерации (Мбайт/сек) для каждого генератора.
   - Зафиксировать время шифрования файла размером 1 Мбайт.
5. Сделать выводы:
   - Какой генератор наиболее криптостойкий.
   - Какой генератор наиболее производительный.
   - Какие генераторы недопустимы для криптографических приложений (и почему).
6. Таблица для сравнения:

Генератор	Период	Скорость (МБ/с)	Статистическая стойкость	Криптостойкость	Рекомендация
LFSR-16	65535	высокая	средняя	низкая (алгоритм Берлекэмпа)	не рекомендуется
LFSR-32	232−1232−1	высокая	средняя	средняя (зависит от полинома)	ограниченно
BBS	теоретически бесконечный	низкая	высокая	высокая (на основе факторизации)	рекомендуется
AES-CTR	21282128	высокая	высокая	высокая	рекомендуется
LCG	m	высокая	низкая	низкая	не рекомендуется

Варианты индивидуальных заданий

№ варианта	Генератор	Параметры	Дополнительное исследование
1	LFSR-16	Полином: $x^{16}+x^5+x^3+x^2+1$	Сравнение с BBS
2	LFSR-32	Полином: $x^{32}+x^7+x^5+x^3+x^2+x+1$	Восстановление состояния
3	BBS	p=83, q=107, n=8881	Сравнение с AES-CTR
4	BBS	p=101, q=103, n=10403	Тесты случайности
5	AES-CTR	Ключ 128 бит	Сравнение с LFSR-32
6	FCSR	q=256	Восстановление состояния
7	LFSR-16	Полином: $x^{16}+x^{12}+x^5+x+1$	Сравнение производительности
8	BBS	p=139, q=167, n=23213	Криптоанализ

РАЗДЕЛ 4. КРИПТОГРАФИЧЕСКИЕ ХЕШ-ФУНКЦИИ

Лабораторная работа №4

Тема: Программная реализация хеш-функции (на примере MD5 или упрощённой версии SHA-256)

Задание 1. Реализация хеш-функции MD5

Реализовать полную версию алгоритма MD5 в соответствии с RFC 1321.

Необходимо:

1. Реализовать вспомогательные функции:
- `left_rotate(x, n)` – циклический сдвиг влево на n бит.
- `F(x, y, z) = (x & y) | (~x & z)`
- `G(x, y, z) = (x & z) | (y & ~z)`
- `H(x, y, z) = x ^ y ^ z`
- `I(x, y, z) = y ^ (x | ~z)`
2. Реализовать функцию дополнения (padding):
- Добавление бита '1'.
- Добавление нулей до длины ≡448(mod 512).
- Добавление 64-битной длины исходного сообщения в битах (little-endian).
3. Реализовать функцию сжатия:
- 4 раунда по 16 операций.
- Использование 16 слов по 32 бита (блок сообщения).
- Использование 16 констант Ki для каждого раунда.
- Обновление состояния (A,B,C,D) после каждого раунда.
4. Реализовать основную функцию:
- `md5(message)` – возвращает 128-битный хеш в виде 32 шестнадцатеричных символов.
5. Реализовать тестовые векторы:
- Пустая строка: `d41d8cd98f00b204e9800998ecf8427e`
- "abc": `900150983cd24fb0d6963f7d28e17f72`
- "message digest": `f96b697d7cb7938d525a2f31aaf161d0`

Задание 2. Реализация упрощённой версии SHA-256

Реализовать упрощённую версию SHA-256 с уменьшенным размером блока и хеша (например, 64-битный хеш) для демонстрации принципов работы.

Варианты:

1. SHA-32: упрощённая версия с 32-битным хешем и 128-битным блоком.
2. SHA-64: упрощённая версия с 64-битным хешем и 256-битным блоком.

Необходимо:

1. Реализовать функции:
- `Ch(x, y, z) = (x & y) ^ (~x & z)`
- `Maj(x, y, z) = (x & y) ^ (x & z) ^ (y & z)`
- `Σ0(x) = ROTR^2(x) ^ ROTR^13(x) ^ ROTR^22(x)`
- `Σ1(x) = ROTR^6(x) ^ ROTR^11(x) ^ ROTR^25(x)`
- `σ0(x) = ROTR^7(x) ^ ROTR^18(x) ^ SHR^3(x)`
- `σ1(x) = ROTR^17(x) ^ ROTR^19(x) ^ SHR^10(x)`
2. Реализовать функцию дополнения:
- Аналогично MD5, но с учётом размера блока.
3. Реализовать функцию сжатия:
- 64 раунда для SHA-32 или 64 раунда для SHA-64.
- Использование констант Kt (первые 32 бита дробных частей кубических корней простых чисел).
- Обновление состояния (H0,H1,...,H7).
4. Реализовать основную функцию:
- `sha256(message)` – возвращает хеш.
5. Провести тестирование:
- Сравнить результаты с известными тестовыми векторами (если реализована полная версия).
- Для упрощённой версии проверить детерминированность и лавинный эффект.

РАЗДЕЛ 5. ЭЛЕКТРОННАЯ ПОДПИСЬ И ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ

Лабораторная работа №5

Тема: Программная реализация схемы ЭП на основе RSA (генерация подписи и верификация)

Задание 1. Генерация ключевой пары RSA

Реализовать программный модуль для генерации ключевой пары RSA с заданной длиной ключа (например, 1024 или 2048 бит).

Необходимо:

1. Реализовать генерацию простых чисел:
- Функция `generate_prime(bits)` – генерация простого числа заданной длины.
- Использовать тест Миллера-Рабина для проверки простоты.
- Обеспечить генерацию чисел p и q с достаточной длиной (например, 512 бит для 1024-битного ключа).
2. Реализовать вычисление ключей:
- Вычисление $n=p \cdot q$.
- Вычисление $\varphi(n)=(p-1)\cdot(q-1)$.
- Выбор $e=65537$ (или другого числа с условием НОД$(e,\varphi(n))=1$).
- Вычисление $d=e^{-1} \bmod \varphi(n)$ с использованием расширенного алгоритма Евклида.
3. Реализовать функции для сохранения и загрузки ключей:
- Сохранение ключей в формате PEM или в виде текстовых файлов.
- Для учебных целей можно использовать JSON или простой текстовый формат.
4. Реализовать функции для преобразования:
- `int_to_bytes(n)` – преобразование целого числа в байтовую строку (big-endian).
- `bytes_to_int(b)` – обратное преобразование.
5. Провести тестирование:
- Сгенерировать ключевую пару.
- Проверить, что d корректно вычислен: $(e \cdot d) \bmod \varphi(n)=1$.
- Проверить шифрование и расшифрование малого числа (для проверки ключей).

Задание 2. Создание и проверка подписи RSA

Реализовать функции для создания и проверки электронной подписи по схеме RSA.

Необходимо:

1. Реализовать функции подписи:
- `sign(message, private_key, hash_func)` – создание подписи.
- `verify(message, signature, public_key, hash_func)` – проверка подписи.
2. Учесть особенности:
- Использование хеш-функции (например, MD5 или SHA-256) для подписи больших сообщений.
- Преобразование хеша в число с учётом размера модуля n.
- Обеспечение, чтобы хеш был меньше n (если хеш больше n, использовать усечение).
3. Реализовать дополнение (padding):
- Простой вариант: добавить к хешу фиксированный заголовок (например, `0x00 0x01` + случайные байты + `0x00` + хеш) – упрощённый аналог PKCS#1 v1.5.
- Для учебных целей можно использовать минимальное дополнение.
4. Реализовать преобразования:
- `os2ip(octet_string)` – преобразование байтовой строки в целое число.
- `i2osp(integer, length)` – преобразование целого числа в байтовую строку фиксированной длины.
5. Провести тестирование:
- Сгенерировать ключи.
- Подписать сообщение.
- Проверить подпись (должна быть корректной).
- Изменить сообщение и проверить подпись (должна быть недействительной).
- Изменить подпись и проверить (должна быть недействительной).

Задание 3. Обработка файлов и работа с большими сообщениями

Расширить программу для работы с файлами и подписи больших сообщений.

Необходимо:

1. Реализовать функции для работы с файлами:
- `sign_file(input_file, output_file, private_key, hash_alg='sha256')` – подписание файла.
- `verify_file(input_file, signature_file, public_key, hash_alg='sha256')` – проверка подписи файла.
2. Учесть особенности:

– Для больших файлов (более нескольких мегабайт) использовать потоковое хеширование (обновление хеша по частям).

– Сохранять подпись в отдельном файле (отсоединённая подпись).

– В учебных целях можно сохранять подпись в формате: `signature.bin` (бинарный файл).

3. Реализовать детектор изменений:

– При проверке подписи выводить сообщение: «Подпись корректна» или «Подпись недействительна (файл изменён)».

4. Реализовать интерфейс командной строки.

5. Провести тестирование:

– Создать текстовый файл.

– Подписать его.

– Проверить подпись (корректно).

– Изменить один байт в файле.

– Проверить подпись (должна быть недействительной).

Варианты индивидуальных заданий

№ варианта	Размер ключа	Хеш-функция	Экспонента e	Дополнительное задание
1	512 бит	SHA-1	3	Демонстрация уязвимости малой экспоненты
2	512 бит	SHA-256	65537	Потоковое хеширование файлов
3	1024 бит	MD5	65537	Демонстрация коллизий MD5
4	1024 бит	SHA-256	17	Подпись и верификация
5	2048 бит	SHA-256	65537	Подпись больших файлов
6	512 бит	SHA-1	65537	Сравнение PKCS#1 и PSS
7	1024 бит	SHA-256	3	Анализ безопасности
8	2048 бит	SHA-512	65537	Реализация PSS

Лабораторная работа №6

Тема: Разработка прототипа системы аутентификации (регистрация, хеширование пароля, вход)

Задание 1. Реализация безопасного хеширования паролей

Реализовать модуль для безопасного хеширования паролей с использованием соли и итеративного хеширования.

Необходимо:

1. Реализовать функции:

– `generate_salt(length=16)` – генерация случайной соли (байтовая строка).

– `hash_password(password, salt, iterations=10000)` – вычисление хеша пароля с солью.

– `verify_password(password, salt, stored_hash, iterations=10000)` – проверка пароля.

2. Реализовать итеративное хеширование:

– Использовать SHA-256 или SHA-512.

– Применять хеш-функцию `iterations` раз: `hash = SHA256(salt + hash)`.

– Увеличить количество итераций для защиты от перебора (рекомендуется ≥ 10000).

3. Реализовать функции для работы с байтами:

– Преобразование хеша и соли в шестнадцатеричный формат для хранения в текстовом виде.

– `to_hex(data)` – преобразование байтов в hex-строку.

– `from_hex(hex_string)` – обратное преобразование.

4. Провести тестирование:

– Сгенерировать соль и хеш для пароля "password123".

– Проверить, что `verify_password("password123", salt, hash)` возвращает True.

– Проверить, что `verify_password("wrong_password", salt, hash)` возвращает False.

– Проверить, что одинаковые пароли с разными солями дают разные хеши.

Задание 2. Реализация системы регистрации и входа

Реализовать прототип системы аутентификации с регистрацией и входом.

Необходимо:

1. Реализовать класс UserManager:

- `register(username, password)` – регистрация нового пользователя.
- `login(username, password)` – вход пользователя.
- `change_password(username, old_password, new_password)` – смена пароля.
- `delete_user(username)` – удаление пользователя.

2. Реализовать хранение данных:

- Хранение в текстовом файле (например, `users.db`) в формате:

username:salt:hash

- Или использование SQLite для более реалистичного примера.

3. Реализовать валидацию паролей:

- Минимальная длина (например, 8 символов).
- Содержание букв, цифр, спецсимволов (по желанию).
- Запрет на использование распространённых паролей (проверка по словарю).

4. Реализовать защиту от атак:

- Ограничение попыток входа (max 5 попыток, затем блокировка на 5 минут).
- Защита от перебора (задержка между попытками).
- Логирование попыток входа.

5. Провести тестирование:

- Зарегистрировать пользователя.
- Войти с корректным паролем.
- Войти с некорректным паролем.
- Проверить блокировку после нескольких неудачных попыток.
- Сменить пароль и войти с новым паролем.

Задание 3. Реализация сессий и защита от атак

Расширить систему аутентификации механизмом управления сессиями и дополнительной защитой.

Необходимо:

1. Реализовать сессионные токены:

- `generate_session_token(username)` – создание случайного токена.
- `validate_session(token)` – проверка валидности токена.
- `logout(token)` – завершение сессии.

2. Реализовать хранение сессий:

- В памяти (для простоты) или в базе данных.
- Установка времени жизни сессии (например, 1 час).
- Автоматическое завершение сессии по истечении времени.

3. Реализовать защиту от CSRF/XSS:

- Использовать http-only cookies для хранения токенов.
- Добавить защиту от подделки межсайтовых запросов.

4. Реализовать логирование событий:

- Регистрация.
- Успешный вход.
- Неудачный вход (с IP-адресом).
- Смена пароля.
- Завершение сессии.

5. Реализовать интерфейс командной строки.

Задание 4. Анализ безопасности и тестирование

Провести анализ безопасности разработанной системы аутентификации.

Необходимо:

1. Провести тестирование на устойчивость к атакам:

- Попытка подбора пароля с использованием словаря.
- Попытка подбора пароля с использованием радужных таблиц (показать, что соль делает их бесполезными).
- Атака повторного воспроизведения (replay attack) – показать, что хеширование защищает.
- DoS-атака на блокировку учётных записей.

2. Проанализировать уязвимости:

- Хранение паролей (соль + хеш).
- Утечка сессионных токенов.
- Отсутствие двухфакторной аутентификации.
- Атаки по времени (timing attacks) при проверке паролей.

3. Предложить улучшения:
- Использование bcrypt/scrypt/Argon2 вместо самодельного хеширования.
- Внедрение двухфакторной аутентификации (TOTP).
- Использование HTTPS для защиты данных при передаче.
- Защита от атак по времени (использование `compare_hashes` с постоянным временем).

4. Сравнить с реальными системами:
- Сравнить с UNIX-системой хранения паролей (`/etc/shadow`).
- Сравнить с системами на основе bcrypt.
- Сравнить с современными стандартами (OWASP рекомендации).

Варианты индивидуальных заданий

№ варианта	Алгоритм хеширования	Итерации	Дополнительное задание
1	SHA-256	10000	Внедрение двухфакторной аутентификации
2	SHA-512	50000	Использование SQLite вместо файлового хранилища
3	SHA-256	100000	Реализация сброса пароля по email
4	SHA-512	10000	Добавление CAPTCHA
5	SHA-256	50000	Логирование в отдельный файл
6	SHA-512	100000	REST API с JWT-токенами
7	SHA-256	10000	Внедрение bcrypt
8	SHA-512	50000	Графический интерфейс (GUI)

ПРИЛОЖЕНИЕ Б

Контрольная работа (5 семестр)

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

1. Почему для криптостойкости важно, чтобы алгоритм шифрования был открыт, а не секретен?

2. Почему частотный анализ эффективен против шифра Цезаря?

3. Какое грубое нарушение правил эксплуатации поточного шифра приводит к расшифровке сообщений злоумышленником?

4. Зачем в блочных шифрах нужны режимы CBC и CTR, если есть простой режим ECB?

5. Для чего в RSA нужны два разных ключа, а не один общий?

6. Почему коллизия считается критической уязвимостью для хеш-функции?

7. Можно ли проверить электронную подпись, имея только закрытый ключ подписавшего?

8. Что произойдёт на этапе аутентификации, если пользователь правильно назвал свой логин, но ввёл неверный пароль?

9. Какую угрозу устраняет сертификат в протоколе TLS на этапе рукопожатия?

10. Что даёт организации аттестат соответствия для объекта информатизации?

11. Почему в блочном шифре нельзя использовать один и тот же ключ для шифрования очень большого объёма данных без смены ключа?

12. Что проверяется на этапе аутентификации после успешной идентификации?

13. Разделите понятия «идентификация» и «аутентификация». Приведите пример трехфакторной аутентификации (перечислите категории факторов).

14. Какие две математические задачи лежат в основе стойкости криптосистемы RSA? Кратко опишите, для чего используется «открытый» ключ, а для чего «закрытый».

15. В чем заключается уязвимость шифра Цезаря и почему он не является стойким? Какой метод криптоанализа наиболее эффективен против него?

Тестовые задания (контрольная работа, 6 семестр)

Индикатор ЗНАТЬ:

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

1. Установите правильную последовательность этапов при шифровании и передаче сообщения с использованием асимметричной криптосистемы.

А) Получатель расшифровывает сообщение своим закрытым ключом

Б) Отправитель шифрует сообщение открытым ключом получателя

В) Отправитель получает от получателя его открытый ключ

Г) Получатель генерирует пару ключей (открытый и закрытый)

2. Установите правильную последовательность действий при создании и проверке электронной подписи.

А) Отправитель шифрует полученный хеш своим закрытым ключом, создавая подпись

Б) Получатель расшифровывает подпись открытым ключом отправителя и получает хеш

В) Отправитель вычисляет хеш-значение документа

Г) Получатель сравнивает полученный хеш с самостоятельно вычисленным хешем документа

3. Установите правильную последовательность этапов процедуры аутентификации по протоколу "вызов-ответ" (Challenge-Response) с использованием симметричного ключа.

А) Система генерирует случайное число (вызов) и отправляет его пользователю

Б) Система сравнивает полученный ответ с эталонным значением

В) Пользователь шифрует полученное число своим секретным ключом и отправляет ответ

Г) Пользователь и система заранее разделяют общий секретный ключ

4. Установите правильную последовательность шагов при атаке злоумышленника на хеш-функцию с целью найти коллизию.

А) Злоумышленник находит два различных сообщения, дающих одинаковый хеш

Б) Злоумышленник выбирает хеш-значение, которое нужно подменить

В) Злоумышленник подменяет одно сообщение другим, сохраняя неизменной его подпись

Г) Злоумышленник анализирует алгоритм хеширования на предмет уязвимостей

5. Установите правильную последовательность обработки данных при шифровании в режиме сцепления блоков (CBC) для блочного шифра.

А) К текущему блоку открытого текста применяется операция исключающего ИЛИ с предыдущим блоком шифротекста

Б) Результат операции шифруется блочным алгоритмом

В) Для первого блока используется случайный инициализирующий вектор

Г) Полученный блок шифротекста сохраняется для использования со следующим блоком

6. Установите правильную последовательность этапов генерации ключей в алгоритме Диффи-Хеллмана.

А) Стороны обмениваются вычисленными значениями по открытому каналу

Б) Алиса и Боб договариваются о двух общих числах (модуль и основание)

В) Каждая сторона вычисляет общий секретный ключ, используя полученное значение другой стороны и свой секретный параметр

Г) Каждая сторона выбирает своё секретное число и вычисляет на его основе открытое значение

7. Установите правильную последовательность мероприятий при аттестации объекта информатизации.

А) Проведение специальных проверок и испытаний средств защиты

Б) Разработка и утверждение модели угроз безопасности информации

В) Выдача аттестата соответствия на объект информатизации

Г) Внедрение сертифицированных средств защиты информации

8. Установите соответствие между криптографическим понятием и его определением.

А) Криптоанализ

Б) Дешифрование

В) Криптостойкость

Г) Ключ

1. Процесс восстановления открытого текста без знания ключа
2. Процесс восстановления открытого текста с использованием известного ключа
3. Секретный параметр, используемый для преобразования данных
4. Свойство алгоритма противостоять попыткам взлома
5. Наука о проектировании криптографических систем

9. Установите соответствие между классическим шифром и его характеристикой.

А) Шифр Цезаря

Б) Шифр Виженера

В) Шифр Плейфера

Г) Шифр Атбаш

1. Использует таблицу букв и ключевое слово для сдвига
2. Заменяет каждую букву на симметричную ей в алфавите
3. Использует фиксированный сдвиг для всех букв
4. Работает с парами букв (биграммами) по таблице 5x5
5. Является шифром перестановки

10. Установите соответствие между типом генератора псевдослучайных чисел (ПСЧ) и его принципом работы.

А) Линейный конгруэнтный генератор

Б) Генератор на основе регистра сдвига с линейной обратной связью (РСЛОС)

В) Криптографически стойкий генератор

Г) Генератор на основе хеш-функции

1. Использует рекуррентную формулу с умножением и сложением
2. Использует сдвиг битов и операцию XOR с отводами
3. Использует итеративное применение хеш-функции к состоянию
4. Обеспечивает непредсказуемость выходной последовательности для злоумышленника
5. Использует только аппаратные источники шума

11. Установите соответствие между режимом работы блочного шифра и его свойством.

А) Режим электронной кодовой книги (ECB)

Б) Режим сцепления блоков (CBC)

В) Режим гаммирования (CTR)

Г) Режим обратной связи по шифротексту (CFB)

1. Требует инициализирующий вектор и делает каждый блок зависимым от предыдущего
2. Одинаковые блоки открытого текста дают одинаковые блоки шифротекста
3. Превращает блочный шифр в поточный с возможностью параллельной обработки
4. Использует обратную связь для самосинхронизации при потере битов
5. Требует дополнения блоков до полного размера

12. Установите соответствие между криптосистемой с открытым ключом и её основным применением или свойством.

А) RSA
Б) Алгоритм Диффи-Хеллмана
В) ECDSA
Г) Алгоритм Эль-Гамаля

1. Используется для генерации электронной подписи на основе эллиптических кривых
2. Используется для безопасного согласования ключа по открытому каналу
3. Основан на сложности факторизации больших чисел
4. Может использоваться как для шифрования, так и для подписи
5. Является симметричным алгоритмом

13. Установите соответствие между хеш-функцией и её характеристикой.

А) MD5
Б) SHA-1
В) SHA-256
Г) CRC32

1. Даёт выходное значение длиной 256 бит
2. Даёт выходное значение длиной 128 бит
3. Даёт выходное значение длиной 160 бит
4. Не является криптографической хеш-функцией, используется для контроля ошибок
5. Является алгоритмом симметричного шифрования

14. Установите соответствие между методом идентификации/аутентификации и его признаком.

А) Аутентификация по паролю
Б) Аппаратный токен
В) Биометрическая аутентификация
Г) Многофакторная аутентификация

1. Основана на уникальных физических характеристиках пользователя
2. Использует комбинацию двух и более различных факторов
3. Является наиболее уязвимым для атак подбора и перехвата
4. Основана на владении физическим устройством, генерирующим одноразовые коды
5. Не требует никаких дополнительных устройств и знаний

15. Установите соответствие между организационной мерой защиты информации и её содержанием.

А) Инструкция по безопасности
Б) Разграничение доступа
В) Аттестация объекта
Г) Резервное копирование

1. Определяет права пользователей на доступ к ресурсам системы
2. Содержит правила поведения и работы с конфиденциальной информацией
3. Предназначено для восстановления данных после сбоя или атаки
4. Подтверждает соответствие объекта установленным требованиям безопасности
5. Осуществляет шифрование всех данных на диске

Индикатор УМЕТЬ:

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

1. Выберете правильный ответ из предложенных вариантов и обоснуйте свой выбор. В чём заключается основное отличие поточного шифра от блочного при обработке данных?

А) Поточный шифр обрабатывает данные блоками фиксированного размера, а блочный – побитово

Б) Поточный шифр шифрует каждый бит или байт отдельно с использованием гаммы, а блочный –

целые блоки

В) Поточный шифр всегда быстрее блочного, но менее надёжен

Г) Поточный шифр не использует ключ, в отличие от блочного

2. Выберете правильный ответ из предложенных вариантов и обоснуйте свой выбор. Какое свойство хеш-функции означает, что невозможно подобрать другое сообщение с таким же хеш-значением, если известно исходное сообщение?

А) Однонаправленность

Б) Стойкость к коллизиям

В) Стойкость к поиску второго прообраза

Г) Детерминированность

3. Выберете правильный ответ из предложенных вариантов и обоснуйте свой выбор. Для чего в электронной подписи используется хеш-функция?

А) Для шифрования всего документа, чтобы его никто не прочитал

Б) Для создания компактного представления документа, которое затем подписывается закрытым ключом

В) Для хранения документа в базе данных

Г) Для проверки полномочий подписывающего лица

4. Выберете правильный ответ из предложенных вариантов и обоснуйте свой выбор. Почему в криптосистемах с открытым ключом закрытый ключ никогда не передаётся по сети?

А) Потому что он слишком длинный

Б) Потому что это делает систему неработоспособной

В) Потому что его перехват позволяет злоумышленнику расшифровывать сообщения или подписываться от имени владельца

Г) Потому что он не нужен для расшифрования

5. Выберете правильный ответ из предложенных вариантов и обоснуйте свой выбор. В чём заключается основная цель аттестации объекта информатизации?

А) Получить разрешение на использование коммерческого программного обеспечения

Б) Официально подтвердить, что уровень защищённости объекта соответствует установленным требованиям

В) Провести инвентаризацию всего оборудования

Г) Обучить сотрудников правилам работы с документами

6. Выберете правильный ответ из предложенных вариантов и обоснуйте свой выбор. Почему при хранении паролей в базе данных используют соль (случайную добавку)?

А) Чтобы пароли занимали больше места

Б) Чтобы усложнить атаку по радужным таблицам и сделать одинаковые пароли разных пользователей неразличимыми в хеше

В) Чтобы зашифровать пароль более стойким алгоритмом

Г) Чтобы пароль можно было восстановить в случае утери

7. Выберете правильный ответ из предложенных вариантов и обоснуйте свой выбор. Какое основное требование предъявляется к генератору псевдослучайных чисел для криптографических целей?

А) Высокая скорость генерации

Б) Непредсказуемость выходной последовательности для злоумышленника

В) Простота реализации на любом языке программирования

Г) Возможность воспроизвести любую сгенерированную последовательность по желанию

Индикатор ИМЕТЬ НАВЫКИ И (ИЛИ) ОПЫТ ДЕЯТЕЛЬНОСТИ

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

1. Прочитайте текст и запишите развернутый ответ. При передаче файла использовался поточный шифр на основе генератора ПСЧ с линейным конгруэнтным методом. Злоумышленник перехватил два разных сообщения, зашифрованные одним и тем же ключом, и знает открытый текст одного из них. Сможет ли он расшифровать второе сообщение и почему?

2. Прочитайте текст и запишите развернутый ответ. В компании хранят резервные копии баз данных на внешнем диске без шифрования. При аттестации эксперты указали это как критическое нарушение. Почему резервные копии должны быть зашифрованы, даже если само помещение с диском охраняется?

3. Прочитайте текст и запишите развернутый ответ. Хеш-функция в системе контроля версий используется для проверки целостности скачанных пакетов. Пользователь скачал файл, вычислил его хеш и сравнил с опубликованным на сайте. Оба значения совпали. Что именно это гарантирует, в отношении безопасности скачанного файла?

4. Прочитайте текст и запишите ответ. Генератор ПСЧ выдаёт 4 байта за такт. Сколько тактов потребуется, чтобы сгенерировать ключ длиной 2048 бит? Разрешается использование калькулятора.

5. Прочитайте текст и запишите ответ. В алгоритме RSA открытая экспонента равна 3, а закрытая – 7. Каково значение модуля, если произведение экспонент при делении на (p-1)(q-1) даёт остаток 1? Разрешается использование калькулятора.

6. Прочитайте текст и запишите ответ. Блочный шифр имеет размер блока 64 бита. Зашифровывается файл размером 5120 бит. Сколько полных блоков будет сформировано? Разрешается использование калькулятора.

7. Прочитайте текст и запишите ответ. В поточном шифре используется гамма длиной 1000 бит. Зашифровано сообщение длиной 800 бит. Сколько бит гаммы осталось неиспользованным? Разрешается использование калькулятора.

8. Прочитайте текст и запишите развернутый ответ. При аттестации объекта выяснилось, что средства криптографической защиты не имеют сертификата ФСБ. Почему наличие такого сертификата является обязательным для государственных информационных систем, и что он подтверждает?

Итоговый тест

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

1. Какая наука является основой для построения большинства современных криптографических алгоритмов с открытым ключом?

А) Математический анализ

Б) Теория чисел

В) Теория вероятностей

Г) Линейная алгебра

2. Какие из перечисленных шифров относятся к классическим (симметричным) шифрам замены?

А) Шифр Вернама

Б) Шифр Цезаря

В) Шифр Виженера

Г) Шифр Энигмы

3. В чем заключается основная проблема использования одноразового блокнота (шифра Вернама) на практике?

А) Низкая криптостойкость

Б) Сложность генерации ключа

В) Необходимость в длинном, полностью случайном и секретном ключе, равном длине сообщения

Г) Невозможность расшифровки на принимающей стороне

4. Какой режим шифрования блочного шифра превращает его в самосинхронизирующийся поточный шифр?

А) Режим электронной кодовой книги (ECB)

Б) Режим сцепления блоков (CBC)

В) Режим счетчика (CTR)

Г) Режим обратной связи по шифротексту (CFB)

5. Какие из перечисленных алгоритмов являются блочными симметричными шифрами?

А) AES

Б) RSA

В) DES

Г) ГОСТ 28147-89 (Magma)

6. Для какой задачи в первую очередь предназначены хеш-функции?

А) Для шифрования больших объемов данных

Б) Для обеспечения целостности данных и создания контрольных сумм

В) Для генерации симметричных ключей

Г) Для цифровой подписи документов

7. Какие из перечисленных свойств обязательны для криптографической хеш-функции?

А) Коллизионная стойкость
Б) Возможность восстановить исходное сообщение по хешу
В) Однонаправленность
Г) Стойкость к поиску второго прообраза

8. Какую функцию в криптосистеме выполняет открытый ключ?
А) Шифрование сообщения для получателя
Б) Расшифрование сообщения, зашифрованного его владельцем
В) Проверка электронной подписи владельца
Г) Создание электронной подписи владельца

9. Какие алгоритмы относятся к криптосистемам с открытым ключом?
А) RSA
Б) Алгоритм Диффи-Хеллмана
В) ECDSA
Г) SHA-256

10. Что является основой для проверки электронной подписи?
А) Закрытый ключ подписывающего
Б) Открытый ключ подписывающего
В) Симметричный ключ сессии
Г) Хеш-значение подписанного документа

11. Какой протокол позволяет пользователю доказать свою подлинность системе, не передавая по сети свой пароль?
А) Протокол одноразовых паролей
Б) Протокол "рукопожатия" на основе симметричного ключа
В) Протокол с нулевым разглашением знания
Г) Протокол вызова-ответа (Challenge-Response)

12. Какие из перечисленных методов используются для аутентификации пользователя?
А) По знанию пароля
Б) По владению аппаратным токеном
В) По биометрическим признакам
Г) По IP-адресу компьютера

13. Какой из перечисленных механизмов предназначен для защиты информации в сетях, обеспечивая конфиденциальность и целостность передаваемых пакетов?
А) Межсетевой экран (Firewall)
Б) Протокол SSL/TLS
В) Антивирусное ПО
Г) Система обнаружения вторжений (IDS)

14. Какие требования предъявляются к организации хранения паролей в базе данных?
А) Пароли должны храниться в открытом виде для быстрого восстановления
Б) Пароли должны храниться в зашифрованном виде с возможностью расшифровки администратором
В) Пароли должны храниться только в виде хеш-значений с использованием соли
Г) Пароли должны передаваться по сети только в открытом виде

15. Какой из этапов является завершающим при аттестации объекта информатизации на соответствие требованиям безопасности?
А) Разработка модели угроз
Б) Установка сертифицированных средств защиты
В) Выдача сертификата соответствия (аттестата) на основании проведенных проверок
Г) Классификация автоматизированной системы