

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.О.22
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

(наименование дисциплины)

по направлению подготовки

01.03.02 Прикладная математика и информатика

направленность (профиль)

Компьютерные технологии и математическое моделирование

Форма обучения: очная

Год набора: 2026

Общая трудоемкость: 4 ЗЕ

Распределение часов дисциплины по семестрам

Семестр	8	Итого
Форма контроля	Экзамен	
Вид занятий		
Лекции	16	16
Лабораторные		
Практические	32	32
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0,35	0,35
Контактная работа	48,35	48,35
Самостоятельная работа	60	60
Контроль	35,65	35,65
Итого	144	144

Рабочую программу составил(и):

Доцент института цифровых технологий, канд. экон. наук. Т.А. Раченко

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана
направления подготовки

01.03.02 Прикладная математика и информатика

Срок действия рабочей программы дисциплины до «31» августа 2030 г.

УТВЕРЖДЕНО

На заседании института цифровых технологий

(протокол заседания № 1 от «05» сентября 2025 г.)

1. Цель освоения дисциплины

Цель – формирование у обучающихся системы теоретических знаний и практических навыков в области обеспечения информационной безопасности, включая защиту информации в распределенных системах, управление жизненным циклом данных, а также применение современных методов и средств защиты информации в профессиональной деятельности.

Задачи:

1. изучить основные понятия, принципы и методы обеспечения информационной безопасности;
2. освоить классификацию угроз информационной безопасности, методы их выявления и противодействия;
3. сформировать умения применять организационные, правовые и технические меры защиты информации;
4. развить навыки анализа рисков и выбора средств защиты для распределенных информационных систем;
5. ознакомиться с нормативно-правовой базой в области защиты информации в Российской Федерации.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.О.22 «Информационная безопасность» относится к обязательной части Блока 1 «Дисциплины (модули)» учебного плана.

Для успешного освоения дисциплины обучающийся должен владеть базовыми знаниями в области:

1. компьютерных сетей (дисциплина Б1.О.23);
2. архитектуры компьютеров и операционных систем (Б1.О.21);
3. баз данных (Б1.О.20);
4. информационных технологий (Б1.О.19).

Знания, умения и навыки, полученные при изучении данной дисциплины, необходимы для выполнения выпускной квалификационной работы (Б3.01(Д)), прохождения преддипломной практики (Б2.В.01(Пд)), а также для профессиональной деятельности в области разработки и эксплуатации защищённых информационных систем.

3. Планируемые результаты обучения

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ПК-8. Способен осуществлять оптимизацию управления жизненным циклом распределенных данных с учетом информационной	ПК-8.1. Знает основы оптимизации управления жизненным циклом распределенных данных, принципы информационной безопасности.	Знать: - основные понятия, принципы и методы обеспечения информационной безопасности; - классификацию угроз информационной безопасности, источники угроз, каналы реализации угроз; - методы и средства защиты информации (криптографические, технические,

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
безопасности		<p>организационные, программно-аппаратные);</p> <ul style="list-style-type: none"> - нормативно-правовые акты в области информационной безопасности РФ; - принципы управления жизненным циклом данных и обеспечения их безопасности в распределенных системах.
	<p>ПК-8.2. Умеет применять методы оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности.</p>	<p>Уметь:</p> <ul style="list-style-type: none"> - выявлять и анализировать угрозы информационной безопасности в информационных системах; - выбирать и обосновывать меры защиты информации в зависимости от класса системы и уровня рисков; - применять основные криптографические методы для защиты конфиденциальности и целостности данных; - использовать средства защиты информации (межсетевые экраны, системы обнаружения вторжений, средства аутентификации и авторизации).
	<p>ПК-8.3. Владеет навыками осуществления оптимизации управления жизненным циклом распределенных данных с учетом информационной безопасности.</p>	<p>Владеть:</p> <ul style="list-style-type: none"> - навыками настройки базовых средств защиты информации (антивирусы, firewall, VPN); - методами оценки уязвимостей и проведения анализа защищенности информационных систем; - технологиями управления жизненным циклом данных с учётом требований информационной безопасности (политики доступа, резервное копирование, шифрование, аудит).

4. Структура и содержание дисциплины

Модуль	Вид учебной работы	Наименование тем занятий	Семестр	Объём, ч	Баллы (max)	Интерактив, ч	Формы текущего контроля
1. Основы криптографической защиты информации	лекция	Тема 1. Введение в информационную безопасность. Основные понятия, угрозы, модели безопасности.	8	2	–	–	–
	лекция	Тема 2. Симметричное шифрование. Алгоритм ТЕА: структура, раунды, константы.	8	2	–	–	–
	Пр	Лабораторная работа №1. Реализация шифрования и дешифрования 64-битного блока данных по алгоритму ТЕА. Генерация 128-битного ключа.	8	4	10	–	Отчёт по ЛР (защита)
	самост.	Изучение лекционного материала, подготовка к лабораторной работе	8	12	–	–	–
2. Режимы шифрования и защита произвольных файлов	лекция	Тема 3. Режимы шифрования (ECB, CBC, OFB). Режим OFB: принцип работы, гаммирование, синхронизация.	8	2	–	–	–
	Пр	Лабораторная работа №2. Шифрование произвольного файла с использованием режима OFB. Обработка неполного последнего блока.	8	6	10	–	Отчёт по ЛР (защита)

Модуль	Вид учебной работы	Наименование тем занятий	Семестр	Объём, ч	Баллы (max)	Интерактив, ч	Формы текущего контроля
	самост.	Разработка алгоритма чтения файла блоками, обработка остатка, подготовка отчёта	8	10	–	–	–
3. Защита ключевой информации. Хэширование	лекция	Тема 4. Криптографические хэш-функции. Алгоритм MD5: структура, раунды, константы. Применение для защиты паролей.	8	2	–	–	–
	Пр	Лабораторная работа №3. Криптосистема с хэшированием пароля (MD5). Генерация ключа сеанса, ввод пароля без отображения, шифрование ключа сеанса ключом от пароля.	8	6	10	–	Отчёт по ЛР (защита)
	самост.	Реализация MD5, изучение методов безопасного ввода пароля, подготовка отчёта	8	12	–	–	–
4. Архивация данных. Алгоритм RLE	лекция	Тема 5. Методы сжатия данных без потерь. Алгоритм RLE: принцип, варианты, кодирование длин серий.	8	2	–	–	–
	Пр	Лабораторная работа №4. Реализация архивации и разархивации файла алгоритмом RLE с кодированием неповторяющихся последовательностей (знаковое число).	8	6	10	–	Отчёт по ЛР (защита)

Модуль	Вид учебной работы	Наименование тем занятий	Семестр	Объём, ч	Баллы (max)	Интерактив, ч	Формы текущего контроля
	самост.	Изучение алгоритма, отладка, подготовка отчёта	8	10	—	—	—
5. Транспортное кодирование. Base64	лекция	Тема 6. Транспортное кодирование. Алгоритм Base64: принцип преобразования 3 байт в 4 символа ASCII, использование символов «=».	8	2	—	—	—
	Пр	Лабораторная работа №5. Реализация транспортного кодирования Base64 для произвольного файла. Обработка неполного блока.	8	4	10	—	Отчёт по ЛР (защита)
	самост.	Реализация функций кодирования/декодирования, подготовка отчёта	8	8	—	—	—
6. Интеграция модулей. Комплексная криптосистема	лекция	Тема 7. Построение комплексных систем защиты информации. Управление через командную строку.	8	2	—	—	—
	Пр	Лабораторная работа №6. Интеграция модулей (архивация, шифрование, транспортное кодирование) в единую криптосистему с выбором режимов через параметры командной строки.	8	6	10	—	Отчёт по ЛР (защита)
	самост.	Сборка модулей, тестирование,	8	12	—	—	—

Модуль	Вид учебной работы	Наименование тем занятий	Семестр	Объём, ч	Баллы (max)	Интерактив, ч	Формы текущего контроля
		подготовка отчёта					
7. Анализ защищённости организации (метод МАРИОН)	лекция	Тема 8. Методика оценки рисков информационной безопасности. Структура метода МАРИОН, анкетирование, расчёт взвешенных сумм, построение диаграмм.	8	2	–	–	–
	Пр	Лабораторная работа №7. Проведение анализа защищённости информационной системы организации (на примере вуза) по методике МАРИОН. Формулирование предложений по снижению рисков, повторный анализ.	8	4	10	–	Отчёт по ЛР (защита)
	самост.	Сбор данных для анкетирования, расчёт показателей, построение диаграмм, подготовка отчёта	8	16	–	–	–
	пром. аттест.	Промежуточная аттестация (экзамен)	8	0,35	30	–	–
Итого				144	100	–	

Схема расчета итогового балла:

Текущий рейтинг (сумма баллов за практические работы) + результат экзамена. Полученная сумма делится на 2. Максимальный итоговый балл – 100. Зачет выставляется при набранном рейтинге 55–100 баллов.

5. Образовательные технологии

В рамках изучения дисциплины «Информационная безопасность» предусмотрено использование следующих образовательных технологий:

- **технология традиционного обучения** (лекции, лабораторные работы) – применяется во всех модулях курса. Лекционные занятия направлены на формирование теоретической базы: изучение принципов криптографии, алгоритмов шифрования, методов защиты информации, нормативно-правовой базы. Лабораторные работы позволяют закрепить теоретические знания на практике, реализуя алгоритмы TEA, OFB, MD5, RLE, Base64, а также интегрируя их в единую криптосистему;
- **интерактивные технологии** – учебные дискуссии, разбор кейсов, работа в малых группах. Используются при обсуждении результатов лабораторных работ, анализе уязвимостей, оценке рисков по методике МАРИОН. В ходе дискуссий обучающиеся представляют свои решения, обсуждают эффективность применённых мер защиты, сравнивают альтернативные подходы. Разбор кейсов (например, анализ атак на модели машинного обучения, оценка последствий SQL-инъекций) позволяет сформировать практические навыки выявления и нейтрализации угроз;
- **проектные технологии** – выполнение практических работ, моделирующих реальные задачи информационной безопасности. В процессе разработки комплексной криптосистемы (лабораторные работы №1–6) обучающиеся создают программный продукт, объединяющий функции шифрования, архивации и транспортного кодирования, что соответствует задачам промышленной разработки защищённых приложений. Анализ защищённости организации по методу МАРИОН (лабораторная работа №7) позволяет обучающимся применить полученные знания к оценке реальной информационной системы, выявить «узкие места» и предложить меры по их устранению.

Применение перечисленных технологий обеспечивает формирование у обучающихся как фундаментальных знаний в области информационной безопасности, так и практических навыков разработки и анализа защищённых систем, необходимых для будущей профессиональной деятельности.

6. Методические указания по освоению дисциплины

6.1 Рекомендации по подготовке к практическим занятиям

Лабораторные работы по дисциплине «Информационная безопасность» направлены на формирование практических навыков реализации криптографических алгоритмов, методов защиты данных и оценки рисков информационной безопасности. Для успешного выполнения работ рекомендуется придерживаться следующего порядка действий:

4. Предварительная подготовка. Перед выполнением каждой лабораторной работы необходимо изучить теоретический материал, представленный в лекциях и рекомендованной литературе. Особое внимание следует уделить:

для ЛР №1–2 – алгоритму TEA, режимам шифрования, принципам гаммирования;

для ЛР №3 – структуре MD5, принципам хэширования и безопасного хранения ключей;

для ЛР №4 – алгоритму RLE, способам кодирования повторяющихся и неповторяющихся последовательностей;

для ЛР №5 – алгоритму Base64, правилам преобразования байтов и дополнения символами «=»;

для ЛР №6 – методам интеграции модулей и управлению через параметры командной строки;

для ЛР №7 – методике МАРИОН, принципам анкетирования, расчёта взвешенных сумм и интерпретации диаграмм.

2. Планирование разработки. Рекомендуется составить план реализации программы, разбив задание на логические этапы (генерация ключа, шифрование блока, обработка файла, обработка неполного блока и т.д.). Для ЛР №6 необходимо предварительно продумать архитектуру объединения ранее написанных модулей и систему обработки параметров командной строки.
3. Разработка и отладка. Код должен быть структурирован, переменные и функции названы с использованием префикса (инициалы студента и символ подчёркивания). Каждый блок кода следует снабжать комментариями, поясняющими назначение переменных и логику работы. В процессе отладки рекомендуется использовать пошаговое выполнение и вывод промежуточных результатов (например, содержимого регистров, значений ключей). Для ЛР №7 полезно предварительно заполнить анкеты на основе открытых сведений об организации и уточнить недостающие данные у преподавателя.
4. Тестирование. Необходимо проверить работоспособность программы на различных наборах данных:

для ЛР №1 – на одном блоке (8 байт) с последующей проверкой корректности дешифрования;

для ЛР №2–6 – на файлах разного размера (включая файлы, размер которых не кратен 8 байтам);

для ЛР №7 – провести расчёт рисков, построить диаграммы и выполнить повторный анализ после внесения предложенных изменений.

5. Оформление отчёта. Отчёт по каждой лабораторной работе должен содержать:
 - титульный лист (по установленному образцу);
 - цель работы;
 - краткие теоретические сведения (основные определения, формулы, описание алгоритмов);
 - описание хода выполнения работы (последовательность действий, листинги кода с комментариями, скриншоты терминала и файлов);
 - результаты работы (полученные зашифрованные/расшифрованные файлы, скриншоты, таблицы с показателями рисков, диаграммы);
 - выводы (достижение цели, анализ эффективности реализованных алгоритмов, обоснование предложенных мер для ЛР №7).

Отчёт должен быть оформлен в текстовом редакторе (шрифт Times New Roman, 14 pt, межстрочный интервал 1,5), все рисунки и таблицы подписаны и пронумерованы. Код и конфигурационные файлы могут быть вынесены в приложения. Отчёт сдаётся преподавателю в электронном виде в установленный срок.

6. Защита лабораторной работы. Защита проводится в форме собеседования, в ходе которого обучающийся должен:

- продемонстрировать работоспособность программы;
- объяснить логику реализации алгоритмов;
- ответить на теоретические вопросы по теме работы;
- обосновать принятые решения (выбор параметров, способ обработки неполных блоков, структуру интеграции модулей и т.д.).

6.2. Рекомендации по подготовке к экзамену

Экзамен по дисциплине «Информационная безопасность» проводится в форме устного или письменного собеседования (по решению преподавателя) с использованием экзаменационных билетов. Каждый билет включает два теоретических вопроса и один практический кейс. Подготовка к экзамену должна носить систематический характер и охватывать следующие направления:

2. Повторение теоретического материала. Рекомендуется использовать конспекты лекций, основную и дополнительную литературу, нормативно-правовые акты (ФЗ-149, ФЗ-152). Особое внимание следует уделить:
 - основным понятиям информационной безопасности (конфиденциальность, целостность, доступность);
 - классификации угроз и моделям нарушителя;
 - принципам симметричного и асимметричного шифрования, режимам шифрования;
 - алгоритмам хэширования и их применению;
 - методам защиты информации (криптографические, организационные, технические);
 - методике оценки рисков МАРИОН.
3. Анализ выполненных лабораторных работ. В процессе подготовки необходимо пересмотреть код и отчёты по всем 7 лабораторным работам, обратив внимание на:
 - алгоритмы, реализованные в каждой работе;
 - типичные ошибки и способы их исправления;
 - особенности обработки неполных блоков данных;
 - логику интеграции модулей в единую криптосистему;
 - полученные результаты анализа рисков и предложенные меры по их снижению.

Самостоятельная проработка вопросов. Вопросы к экзамену охватывают весь курс, включая темы, выходящие за рамки лабораторных работ (например, правовые аспекты, организационные меры, современные направления защиты данных). При подготовке рекомендуется составлять краткие конспекты ответов, выделяя ключевые определения, классификации и примеры.

Время подготовки и порядок ответа. На подготовку к ответу отводится 35 минут. В это время можно составить план ответа, выписать формулы, схемы, ключевые термины. Ответ должен быть логичным, научно обоснованным, с опорой на теоретические положения и практический опыт выполнения лабораторных работ. После ответа на вопросы билета преподаватель может задать уточняющие и дополнительные вопросы по всему курсу.

Систематическая работа в течение семестра (выполнение всех лабораторных работ, участие в обсуждениях, своевременное повторение материала) позволит использовать время экзаменационной сессии для систематизации знаний и успешно сдать экзамен.

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
8	ПК-8	Вопросы к экзамену, Отчёты по лабораторным работам №1–7

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Отчеты по лабораторным работам

(наименование оценочного средства)

Типовые задания для текущего контроля

Лабораторная работа №1. Реализация шифрования ТЕА для 64-битного блока данных

Цель работы: освоить алгоритм ТЕА, научиться шифровать и дешифровать один блок данных.

Задание:

- Разработать программу на языке программирования, которая:
 - генерирует 128-битный ключ (4×32 бита) с помощью псевдослучайной функции;
 - сохраняет ключ в файл key.txt (16 байт);
 - считывает из входного файла 8 байт (64 бита);
 - шифрует блок по алгоритму ТЕА;
 - сохраняет зашифрованный блок в выходной файл с расширением .enc;
 - выполняет дешифрование и сравнивает результат с исходным блоком.
- Исходный код должен содержать комментарии, имена переменных и функций должны начинаться с инициалов студента и символа подчёркивания (например, КАВ_encrypt).
- Предусмотреть запуск программы с параметрами: -e (шифрование) и -d (дешифрование) с указанием имён файлов.
- Подготовить отчёт с листингом программы, скриншотами запуска и результатами.

Лабораторная работа №2. Шифрование произвольного файла в режиме OFB

Цель работы: научиться применять режим OFB для поточного шифрования файлов произвольного размера.

Задание:

1. Модифицировать программу из ЛР №1 для шифрования файла любого размера в режиме OFB (гаммирование).
2. Использовать 64-битный вектор инициализации (IV), который генерируется случайно и записывается в начало зашифрованного файла.
3. Реализовать чтение файла блоками по 4 байта (32 бита), гаммирование с использованием предварительно зашифрованного регистра.
4. Обработать неполный последний блок (дополнить нулями).
5. При дешифровании считать IV из начала файла, восстановить гамму и расшифровать данные.
6. Проверить работоспособность на файле размером не менее 4 Мб, не кратном 8 байтам.
7. Оформить отчёт с кодом, скриншотами и описанием.

Лабораторная работа №3. Криптосистема с хэшированием пароля и ключом сеанса

Цель работы: освоить методы защиты ключевой информации с помощью хэш-функции.

Задание:

1. Реализовать хэш-функцию MD5 / SHA 256 для получения ключа из пароля пользователя.
2. Организовать ввод пароля без отображения на экране.
3. Сгенерировать случайный 128-битный ключ сеанса (сеансовый ключ).
4. Зашифровать ключ сеанса ключом, полученным из пароля (путём XOR или с использованием TEA).
5. Зашифровать исходный файл с помощью режима OFB и ключа сеанса (как в ЛР №2).
6. В конец зашифрованного файла добавить зашифрованный ключ сеанса.
7. При дешифровании: считать из файла зашифрованный ключ сеанса, расшифровать его паролем пользователя, затем расшифровать основную часть файла.

8. Оформить отчёт с кодом, скриншотами ввода пароля и результатами.

Лабораторная работа №4. Архивация данных алгоритмом RLE

Цель работы: изучить метод сжатия RLE и реализовать его для произвольного файла.

Задание:

1. Реализовать программу архивации и разархивации файла с использованием алгоритма RLE (Run-Length Encoding).
2. Правила кодирования:
 - для последовательности из 3–127 одинаковых символов: записывается положительное число (длина) и один символ;
 - для последовательности из 1–128 неповторяющихся символов: записывается отрицательное число (длина, со знаком минус) и затем сама последовательность.
3. При повторении символов менее 3 раз кодировать как неповторяющиеся.
4. Выходной файл при архивации получает расширение `.arh`. При разархивации расширение отбрасывается; если файл с исходным именем уже существует, к имени добавляется (1).
5. Проверить, что разархивированный файл идентичен исходному.
6. Оформить отчёт с кодом, скриншотами и описанием.

Лабораторная работа №5. Транспортное кодирование Base64

Цель работы: освоить алгоритм Base64 для преобразования бинарных данных в печатные ASCII-символы.

Задание:

1. Реализовать функции кодирования и декодирования произвольного файла по алгоритму Base64.
2. Для кодирования: разбить входной поток на группы по 3 байта, преобразовать в 4 символа из таблицы A–Z, a–z, 0–9, +, /.
3. Если последняя группа содержит менее 3 байт, дополнить её нулями, а в выходной строке добавить символы = в соответствии с количеством недостающих байт.

4. Сохранить результат в файл с расширением .trans.
5. При декодировании: восстановить исходные данные, игнорируя символы = и преобразуя символы обратно в 6-битные группы.
6. Проверить, что декодированный файл идентичен исходному.
7. Оформить отчёт с кодом, скриншотами и описанием.

Лабораторная работа №6. Интеграция модулей в единую криптосистему

Цель работы: создать комплексную программу, объединяющую ранее разработанные модули с возможностью выбора операций через параметры командной строки.

Задание:

1. Разработать единую программу, которая объединяет функциональность:
 - архивации RLE (ЛР №4);
 - шифрования TEA в режиме OFB с ключом сеанса (ЛР №2 и №3);
 - транспортного кодирования Base64 (ЛР №5).
2. Реализовать параметры командной строки:
 - -e – шифрование (последовательное применение: архивация → шифрование → Base64);
 - -d – дешифрование (обратный порядок);
 - -a – включить архивацию;
 - -t – включить транспортное кодирование;
 - -k – использовать ключ сеанса (в противном случае ключ генерируется из пароля).
3. Программа должна корректно обрабатывать любую комбинацию параметров (например, только шифрование, шифрование с архивацией, полная цепочка).
4. При дешифровании необходимо автоматически определять применённые операции (по расширениям файлов) и восстанавливать исходный файл.
5. Оформить отчёт с кодом, скриншотами работы с разными параметрами и проверкой корректности восстановления.

Лабораторная работа №7. Анализ защищённости организации методом МАРИОН

Цель работы: научиться проводить оценку рисков информационной безопасности по методике МАРИОН и формулировать предложения по снижению рисков.

Задание:

1. На основе предоставленных анкет (секции 1–6) провести анализ защищённости информационной системы организации (на примере университета).
2. Для каждого вопроса выставить оценку (от 0 до 4) в соответствии с реальным положением дел.
3. Рассчитать взвешенные суммы по каждому фактору и каждой секции.
4. Построить:
 - диаграмму КИВИАТ (розу рисков), отображающую защищённость по каждому фактору;
 - дифференциальную диаграмму, показывающую отклонение от идеального уровня (риск = 0).
5. На основе выявленных рисков сформулировать основные направления защиты информации (не менее 5 предложений).
6. Провести повторный анализ после внедрения предложенных мер, рассчитать новые показатели рисков и построить диаграммы.
7. Убедиться, что уровень рисков по всем направлениям не превышает заданного (выбирается студентом самостоятельно, например, 30% от максимального).
8. Оформить отчёт с заполненными анкетами, расчётами, диаграммами до и после, выводами и предложениями.

Общие требования к оформлению отчётов

1. Отчёт по каждой лабораторной работе выполняется в текстовом редакторе (шрифт Times New Roman, 14 pt, межстрочный интервал 1,5, поля – 2 см) и сдаётся преподавателю в электронном виде (PDF или DOCX).
2. По каждой работе создаётся отдельный отчёт.
3. Обязательные структурные элементы отчёта:
 - титульный лист (оформляется по установленному образцу);
 - цель работы (формулируется в соответствии с заданием);
 - краткие теоретические сведения (основные определения, формулы, описание алгоритмов);
 - описание хода выполнения работы (последовательность действий, используемые инструменты, листинги кода с комментариями, скриншоты терминала и файлов);
 - результаты выполненной работы (полученные данные, скриншоты, таблицы, диаграммы, числовые значения);
 - выводы (краткий анализ полученных результатов, достижение цели работы).
4. Все рисунки и таблицы должны иметь подписи и номера (например, *Рисунок 1 – Содержимое входного файла, Таблица 1 – Результаты расчёта рисков*).
5. Код программ и конфигурационные файлы могут быть вынесены в приложения. Приложения включаются в общую нумерацию страниц.

Критерии оценки отчётов по лабораторным работам

Максимальный балл за каждую лабораторную работу – **10**. Оценка производится по следующей шкале:

Баллы	Характеристика выполнения и защиты
10	Работа выполнена в полном объёме с соблюдением необходимой последовательности действий. Отчёт оформлен аккуратно, без ошибок. Вывод исчерпывающий и доказательный . При защите студент ответил на все вопросы по теме, хорошо ориентируется в материале, умеет обосновать принятые решения.
7–9	Работа выполнена в полном объёме , отчёт выполнен без ошибок, вывод исчерпывающий. При защите студент хорошо разбирается в материале , но не уверен и неполно отвечает на вопросы. Способность к обобщению выражена недостаточно.
4–6	Работа выполнена не полностью , но объём выполненной части позволяет получить правильные результаты и выводы. Работа выполнена с несущественными замечаниями . Вывод по работе не раскрывает сути работы . Владение понятийным аппаратом недостаточное .
1–3	Студент выполнил работу не полностью или объём выполненной части не позволяет сделать правильных выводов . В ответах на вопросы есть грубые ошибки . Нет знания принципиальных теоретических положений темы.
0	Работа не сдана или не представлена к защите.

Допуск к экзамену – успешное выполнение и защита всех 7 лабораторных работ (оценка не ниже «удовлетворительно»).

7.3 Вопросы к промежуточной аттестации (экзамену)

Модуль 1. Основы криптографической защиты информации (вопросы 1–15)

1. Дайте определение информационной безопасности. Перечислите основные цели защиты информации (конфиденциальность, целостность, доступность).
2. Классифицируйте угрозы информационной безопасности по природе возникновения, источнику и последствиям.
3. Что такое модель нарушителя? Какие виды нарушителей выделяют в информационных системах?
4. Опишите алгоритм TEA (Tiny Encryption Algorithm). Какова структура раунда, какие константы используются?
5. Почему в алгоритме TEA используется 32 раунда? Какое значение имеет константа 0x9e3779b9?
6. Объясните принцип работы режима OFB (Output Feedback). В чем его преимущества перед ECB и CBC?
7. Как обеспечивается синхронизация при использовании режима OFB? Что такое вектор инициализации (IV)?
8. Каким образом обрабатывается последний неполный блок при шифровании файла в режиме OFB?

9. В чем отличие симметричного шифрования от асимметричного? Приведите примеры алгоритмов.

10. Что такое криптостойкость? Какие факторы влияют на стойкость алгоритма TEA?

11. Опишите порядок генерации 128-битного ключа в лабораторной работе №1. Какие функции генерации случайных чисел использовались?

12. Какие требования предъявляются к ключам шифрования? Почему не рекомендуется использовать простые или повторяющиеся ключи?

13. Что такое «соль» (salt) и где она применяется в криптографии?

14. Какие режимы шифрования позволяют выполнять параллельную обработку блоков, а какие – нет?

15. Объясните принцип гаммирования. Как режим OFB реализует гаммирование?

Модуль 2. Защита ключевой информации. Хэширование (вопросы 16–25)

16. Что такое хэш-функция? Перечислите основные свойства криптографических хэш-функций.

17. Опишите структуру алгоритма MD5. Сколько раундов, какие константы используются?

18. Для каких целей применяется MD5? Какие недостатки этого алгоритма известны?

19. Как в лабораторной работе №3 реализовано получение ключа шифрования из пароля? Почему пароль не хранится в файле?

20. Каким образом обеспечивается ввод пароля без отображения на экране? Какие функции для этого использовались?

21. Что такое ключ сеанса? Как он генерируется и где хранится в зашифрованном файле?

22. Объясните процедуру шифрования ключа сеанса ключом, полученным из пароля. Почему это необходимо?

23. Какие существуют методы защиты от подбора пароля (brute-force)? Как усложнить задачу злоумышленнику?

24. Что такое «солёный» хэш? Как это может быть применено к хранению паролей?

25. Сравните алгоритмы MD5, SHA-1, SHA-256. Какие из них сегодня считаются криптостойкими?

Модуль 3. Архивация данных. Алгоритм RLE (вопросы 26–32)

26. Что такое сжатие данных без потерь? Приведите примеры алгоритмов.

27. Опишите принцип работы алгоритма RLE (Run-Length Encoding). В каких случаях он эффективен?

28. Каким образом в лабораторной работе №4 кодируются неповторяющиеся последовательности? Почему используется знаковое число?

29. Как обрабатываются последовательности длиной 2 одинаковых символа? Объясните логику выбора между кодированием как повторяющихся и как неповторяющихся.

30. Какие ограничения на длину последовательностей заданы в работе (положительные и отрицательные числа)? Почему выбраны именно эти пределы?

31. Как в алгоритме RLE обеспечивается восстановление исходного файла? Какие данные сохраняются в архив?

32. В каких типах файлов (текстовые, графические, исполняемые) RLE даёт наибольшее сжатие? Обоснуйте.

Модуль 4. Транспортное кодирование. Base64 (вопросы 33–40)

33. Для чего используется транспортное кодирование? Приведите примеры применения Base64.

34. Опишите принцип преобразования 3 байт в 4 символа Base64. Как формируется таблица символов?

35. Каким образом обрабатываются неполные блоки (1 или 2 байта)? Что означает символ = в конце строки?

36. В чем отличие между стандартной таблицей Base64 и URL-safe вариантом?

37. Какие недостатки имеет Base64 с точки зрения увеличения объёма данных? Во сколько раз увеличивается размер?

38. В лабораторной работе №5 какие операции выполняются при декодировании? Как восстанавливаются исходные байты?

39. Какие алгоритмы транспортного кодирования, кроме Base64, вы знаете? (Base32, Base16, Quoted-Printable)

40. Почему Base64 широко используется в электронной почте (MIME) и при передаче данных в JSON/XML?

Модуль 5. Интеграция модулей. Комплексная криптосистема (вопросы 41–50)

41. Опишите архитектуру комплексной криптосистемы, разработанной в лабораторной работе №6. Какие модули объединены?

42. Какие параметры командной строки поддерживаются программой? Как они влияют на последовательность операций?

43. Почему при шифровании рекомендуется сначала архивировать, затем шифровать, а затем применять транспортное кодирование? Какой порядок при дешифровании?

44. Как в программе обрабатывается случай, когда указаны не все параметры (например, только -e без -a и -t)?

45. Какие расширения файлов используются для обозначения архивированных, зашифрованных и закодированных данных?

46. Как реализовано восстановление исходного имени файла при дешифровании? Что происходит при возникновении конфликта имён?

47. Какие преимущества даёт использование ключа сеанса по сравнению с непосредственным шифрованием паролем?

48. Как в интегрированной программе обеспечивается проверка целостности данных? Какие механизмы можно добавить?

49. Какие дополнительные меры безопасности можно добавить в разработанную криптосистему (например, аутентификацию сообщений, цифровую подпись)?

50. Какие ошибки могут возникнуть при интеграции модулей и как их можно отладить?

Модуль 6. Анализ защищённости организации (метод МАРИОН) (вопросы 51–60)

51. Что такое метод МАРИОН? Кем и для каких целей он был разработан?

52. Опишите структуру анкеты метода МАРИОН. Какие разделы (секции) входят в опросный лист?

53. Что такое «фактор» в методике МАРИОН? Как рассчитывается взвешенная оценка по фактору?

54. Как интерпретируется диаграмма КИВИАТ (роза рисков)? Что означает большая площадь диаграммы?

55. Что показывает дифференциальная диаграмма? Как определяется идеальный уровень риска?

56. Какие факторы относятся к секции 3 «Общая компьютерная безопасность»? Приведите примеры вопросов.

57. Как в методе МАРИОН учитываются социоэкономические факторы? Приведите примеры.

58. Каким образом проводится повторный анализ после внесения предложенных изменений?

59. Какие основные направления защиты информации можно выработать на основе анализа рисков?

60. Какие современные методы оценки рисков, кроме МАРИОН, вы знаете? (ГОСТ Р 57580, NIST SP 800-30)

7.3.2. Критерии и нормы оценки (экзамен)

Промежуточная аттестация по дисциплине «Информационная безопасность» проводится в форме **экзамена**. Экзамен проводится в устной или письменной форме (по решению преподавателя) с использованием экзаменационных билетов. Каждый билет содержит **два теоретических вопроса**.

Процедура проведения экзамена

1. На подготовку к ответу отводится **30 минут**.
2. В процессе подготовки разрешается составлять краткий план ответа, выписывать ключевые определения, формулы, схему решения кейса.
3. После подготовки экзаменуемый последовательно излагает ответы на вопросы билета.
4. Преподаватель может задавать уточняющие и дополнительные вопросы как по содержанию билета, так и по всему курсу.

Требования к ответу

1. Ответ должен быть научным, логически стройным и опираться на соответствующие теоретические положения, а также на практический опыт выполнения лабораторных работ.
2. Необходимо строить ответ в единстве теории и практики, подкрепляя теоретические положения примерами из выполненных лабораторных работ.
3. При ответе на теоретические вопросы следует чётко формулировать определения, классификации, перечислять методы и инструменты, объяснять принципы их работы.

Критерии оценки ответа на экзамене

Оценка	Критерии
«отлично»	Обучающийся полностью раскрыл содержание всех вопросов билета: даны исчерпывающие, аргументированные ответы, демонстрирующие глубокое понимание материала. Ответ логичен, грамотен, структурирован. На дополнительные вопросы даны правильные ответы.
«хорошо»	Обучающийся полностью раскрыл содержание всех вопросов билета, но допустил незначительные неточности или недостаточно полно аргументировал отдельные положения. На дополнительные вопросы ответил правильно, но с некоторыми затруднениями.
«удовлетворительно»	Обучающийся раскрыл содержание вопросов билета в минимально необходимом объёме, допустил отдельные ошибки, которые исправил после наводящих вопросов. На дополнительные вопросы ответил неуверенно.
«неудовлетворительно»	Обучающийся не раскрыл содержание вопросов билета, допустил принципиальные ошибки. Не может ответить на дополнительные вопросы.

Обучающийся, получивший на экзамене оценку «неудовлетворительно», направляется на пересдачу в установленном порядке.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно-методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Раченко, Т.А.	Учебно-методическое пособие «Информационная безопасность»	Учебно-методическое пособие	2024	Репозиторий ТГУ
2	Бондаренко, И. С.	Информационная безопасность : учебник / И. С. Бондаренко. - Москва : Издательский Дом НИТУ «МИСиС», 2023. - 255 с. - ISBN 978-5-907560-71-0.	Учебник	2023	ЭБС «Znanium»
3	Суворова, Г. М.	Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 с. — ISBN 978-5-4487-1026-1.	Учебное пособие	2024	ЭБС “IPRbooks”

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
4	Рубин, Ф.	Криптография с секретным ключом : практическое руководство / Ф. Рубин ; пер. с англ. А. А. Слинкина. - Москва : ДМК Пресс, 2023. - 386 с. - ISBN 978-5- 97060-748-0.	Практическое руководство	2023	ЭБС «Znanium»
5	Бирн, Д.	Безопасность веб-приложений на Python. Криптография, TLS и устойчивость к атакам : практическое руководство / Д. Бирн ; пер. с англ. С. С. Скобелева, А. Н. Киселева. – Москва : ДМК Пресс, 2021. - 336 с. – ISBN 978-5-97060-899-9.	Практическое руководство	2021	ЭБС «Znanium»

8.3. Перечень профессиональных баз данных и информационных справочных систем

№ пп	Наименование	Ссылка
1	ЭБС «Лань»	ЭБС Лань
2	ЭБС "ZNANIUM.COM"	Электронно-библиотечная система Znanium
3	ЭБС "IPRbooks"	IPR SMART / Главная
4	Портал ФСТЭК России (нормативные документы по защите информации)	https://fstec.ru/
5	Портал «Информационная безопасность» (аналитика, новости, стандарты)	https://www.securitylab.ru/
6	CVE Details (база данных известных уязвимостей)	https://www.cvedetails.com/
7	OWASP Foundation (безопасность веб-приложений, уязвимости, инструменты)	https://owasp.org/
8	CryptoPro (криптографическая защита информации)	https://www.cryptopro.ru/

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Среда разработки Code:Blocks	Свободное ПО (лицензия GPL)
2	Среда разработки Visual Studio Code	Свободное ПО (лицензия MIT)
3	Компилятор MinGW (GCC)	Свободное ПО (лицензия GPL)
4	Язык программирования C++ (стандартные библиотеки)	Свободное ПО
5	OpenSSL (библиотека криптографии)	Свободное ПО (лицензия Apache 2.0)

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
6	Python (для анализа данных в ЛР №7)	Свободное ПО (лицензия PSF)
7	Библиотеки Python: pandas, matplotlib, numpy (для построения диаграмм)	Свободное ПО (лицензии BSD, MIT)
8	Adobe Acrobat Reader (просмотр PDF)	Бесплатное ПО
9	Git (система контроля версий)	Свободное ПО (лицензия GPL)
10	Wireshark (анализ сетевого трафика – для дополнительного изучения)	Свободное ПО (лицензия GPL)
11	Nmap (сканирование сети – для дополнительного изучения)	Свободное ПО (лицензия GPL)
12	SQLite / PostgreSQL (для работы с базами данных – по желанию)	Свободное ПО (лицензия Public Domain / PostgreSQL License)

8.5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
1	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для проведения лабораторных работ. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. (УЛК-408)	Компьютер, проектор Acer P1303W., стол преподавательский, стол ученический, стол компьютерный, стул, доска аудиторная (маркерная).
2	Компьютерный класс. Помещение для самостоятельной работы. Учебная аудитория	Столы ученические, стулья ученические, ПК с выходом в сеть

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации (Г-401)	Интернет