МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по дисциплине
«Перспективные направления защиты информации»
для студентов
Специальности 10.05.03 Информационная безопасность автоматизированных систем Специализация «Анализ безопасности информационных систем»

Ставрополь
2026

Лабораторная работа 1

Знакомство с современными угрозами информационной безопасности и средствами их нейтрализации.

Цель работы:
Изучить современные виды угроз информационной безопасности, их характерные черты и тенденции развития. Ознакомиться с методами, подходами и средствами их нейтрализации. Сформировать понимание перспектив развития киберугроз и глобальных вызовов в области информационной безопасности.

Теоретическая часть

1. Актуальность темы

Информационная безопасность — это одно из ключевых направлений в сфере цифровой трансформации общества. В условиях глобальной цифровизации и массового внедрения ИТ-решений возрастает не только количество информационных ресурсов, но и потенциальных точек уязвимости. Современные угрозы становятся всё более разнообразными, комплексными и высокотехнологичными, охватывая не только технические, но и социальные, организационные аспекты.

2. Классификация современных угроз информационной безопасности

Современные угрозы можно условно разделить на несколько групп:
– вредоносное ПО (вирусы, трояны, шифровальщики, ботнеты);
– атаки на отказ в обслуживании (DoS/DDoS);
– утечки данных (в том числе через инсайдеров);
– фишинг, социальная инженерия и мошенничество;
– уязвимости в программном обеспечении;
– атаки на инфраструктуру (включая IoT и SCADA-системы);
– кибершпионаж, кибервойны и атаки на уровне государств.

3. Тенденции развития киберугроз

Современные угрозы приобретают следующие особенности:
– активное использование ИИ и машинного обучения в кибератаках;
– рост количества атак на цепочки поставок ПО;
– применение zero-day уязвимостей;
– широкое распространение киберпреступности как "услуги" (Cybercrime-as-a-Service);
– геополитическая мотивация атак, рост числа государственно-спонсируемых группировок.

4. Средства и методы нейтрализации угроз
Ключевые подходы к защите от современных угроз:
– внедрение многоуровневых систем защиты (модель Zero Trust, концепция Defense in Depth);
– регулярное обновление ПО и патч-менеджмент;
– мониторинг и анализ поведения в сети (SIEM, XDR, NDR-системы);
– использование средств защиты от вредоносного ПО нового поколения;
– шифрование данных и управление ключами;
– проведение аудитов и тестов на проникновение;
– повышение уровня осведомлённости пользователей (обучение, симуляции фишинга).

5. Перспективные угрозы и вызовы будущего
Среди возможных угроз будущего выделяются:
– атаки на квантовые вычислительные системы;
– использование генеративного ИИ для обхода систем защиты;
– взлом и подмена биометрических данных;
– атаки на нейронные сети и системы автономного управления;
– эксплойты в метавселенных и киберфизических системах.
Также стоит ожидать роста атак на критически важную инфраструктуру, усиления информационного противоборства и эволюции кибероружия.

Вопросы для обсуждения

1. Какие современные угрозы ИБ являются наиболее опасными для бизнеса и государства?
2. В чём заключается разница между киберпреступностью и кибершпионажем?
3. Как изменились методы защиты от фишинга и социальной инженерии за последние годы?
4. Почему важно учитывать человеческий фактор при построении системы ИБ?
5. Какие технологии играют ключевую роль в обнаружении и нейтрализации угроз в реальном времени?
6. Что такое концепция Zero Trust и как она реализуется на практике?
7. Какие угрозы могут возникнуть в связи с развитием квантовых вычислений?
8. Как государственные структуры и международные организации реагируют на рост киберугроз?
9. Какие примеры глобальных атак последних лет вы можете привести? Каковы их последствия?
10. Какие профессиональные компетенции становятся наиболее важными в сфере кибербезопасности будущего?

Практическая часть

Задание 1. Анализ кейса реальной кибератаки.
Выберите одну из известных кибератак (например: SolarWinds, WannaCry, Colonial Pipeline, атака на DNC и др.). Подготовьте краткий доклад, включающий:
– общие сведения об атаке;
– цели и средства нападения;
– последствия атаки;
– методы защиты и реагирования, применённые в ответ.

Задание 2. Классификация угроз.
Создайте таблицу, в которую включите 5–7 современных угроз ИБ. Укажите для каждой из них: источник, тип атаки, цель, методы нейтрализации, примеры инцидентов.

Задание 3. Сравнительный анализ подходов к защите.
Сравните традиционный периметральный подход к информационной безопасности и концепцию Zero Trust. Представьте результат в виде таблицы с указанием ключевых различий, преимуществ и недостатков.

Задание 4. Прогноз угроз.
Ознакомьтесь с докладами организаций (например, ENISA, Kaspersky, Mandiant, Gartner) о прогнозах киберугроз. Подготовьте сводку о предполагаемых направлениях атак на ближайшие 3–5 лет и возможных способах противодействия.

Задание 5. Оценка уровня защищённости.
Смоделируйте гипотетическую организацию (например, небольшая IT-компания). Опишите её ИТ-инфраструктуру и оцените уязвимые точки. Предложите базовый набор мер защиты от современных угроз.

Задание 6. Разработка краткой стратегии ИБ.
Сформулируйте краткий план информационной безопасности организации, включающий ключевые направления: управление рисками, мониторинг, обучение персонала, реагирование на инциденты, резервное копирование.

Ожидаемые результаты:
В результате выполнения лабораторной работы студент:
– освоит классификацию современных угроз информационной безопасности;
– получит знания о наиболее эффективных средствах их нейтрализации;
– научится анализировать кибератаки и делать выводы о методах защиты;
– ознакомится с глобальными тенденциями развития киберугроз;

– сможет предложить первичные меры защиты для конкретных случаев и организаций.

Форма отчета:
– Титульный лист
– Краткое описание теоретической части
– Ответы на вопросы
– Выполненные практические задания
– Выводы и рекомендации

Рекомендуемая литература и ресурсы:

1. Сетевые отчёты и прогнозы (ENISA Threat Landscape, Verizon DBIR, Kaspersky Security Bulletin)
2. Стандарты и методики: ISO/IEC 27001, NIST Cybersecurity Framework
3. Онлайн-ресурсы: ThreatPost, BleepingComputer, MITRE ATT&CK
4. Учебники по ИБ: Блюм, С. "Основы информационной безопасности", Киселев А.В. "Информационная безопасность: современные угрозы и защита"

Лабораторная работа 2

Анализ методов квантовой криптографии и моделирование квантовой передачи ключей. Основы квантовой защиты информации и её потенциал

Цель работы:
Ознакомиться с основами квантовой криптографии как перспективного направления в защите информации. Изучить принципы работы квантовой передачи ключей (QKD), их физические основы и протоколы реализации. Провести анализ потенциальных возможностей и ограничений квантовой защиты в условиях развития квантовых вычислений.

Теоретическая часть

1. Актуальность квантовой криптографии

С развитием квантовых технологий появляется угроза взлома традиционных криптографических алгоритмов, таких как RSA, ECC и другие, основанные на математических задачах, легко решаемых квантовыми компьютерами (например, с помощью алгоритма Шора). В этих условиях квантовая криптография становится одним из наиболее перспективных направлений, обеспечивающих информационную безопасность в постквантовую эпоху.

2. Основы квантовой защиты информации
Квантовая криптография использует законы квантовой физики для обеспечения безопасности связи. Основные принципы:
– **Квантовое состояние не может быть измерено без его искажения (принцип неопределённости Гейзенберга)**
– **Копирование неизвестного квантового состояния невозможно (теорема о запрете клонирования)**
– **Наличие подслушивающего всегда может быть зафиксировано**
Это позволяет реализовать абсолютно безопасную передачу криптографических ключей между сторонами.

3. Протоколы квантовой передачи ключей (QKD)
Наиболее известным и используемым протоколом является **BB84** (предложен Беннетом и Брассаром в 1984 году). Другие примеры: **E91 (Экерт, 1991)**, **B92**, **SARG04**.
Кратко о протоколе BB84:
– Используются два базиса поляризации фотонов: прямой (+) и диагональный (×).
– Отправитель (Алиса) случайным образом кодирует биты и отправляет их в виде фотонов.
– Получатель (Боб) также случайно выбирает базис для каждого фотона.
– Совпадающие измерения формируют секретный ключ.
– Наличие подслушивания проверяется через сравнение части битов на целостность.

4. Аппаратные и программные аспекты
Реализация квантовой передачи требует наличия квантовых каналов (обычно — оптоволоконная линия или свободное пространство), источников одиночных фотонов, квантовых детекторов и синхронизирующего оборудования. Существуют также симуляторы и ПО для моделирования QKD (например, QuTiP, SimulaQron).

5. Потенциал и вызовы квантовой защиты
Преимущества:
– Безусловная безопасность (при корректной реализации)
– Защита от атак с использованием квантовых компьютеров
Ограничения:
– Ограниченная дальность передачи (до 300 км по оптоволокну без повторителей)
– Сложность и дороговизна оборудования
– Сложности с интеграцией в существующие сети
Будущее квантовой защиты связано с развитием **квантового Интернета**, квантовых ретрансляторов, спутниковых квантовых сетей.

Вопросы для обсуждения

1. В чём принципиальное отличие квантовой криптографии от классических методов шифрования?
2. Как работает протокол BB84? Опишите последовательность действий отправителя и получателя.
3. Почему квантовую передачу ключей нельзя подслушать, не вызвав ошибок?
4. Какие физические принципы лежат в основе квантовой защиты информации?
5. Какие перспективы и ограничения существуют у QKD в реальных условиях?
6. Какие существуют альтернативные протоколы, кроме BB84?
7. Можно ли использовать квантовую криптографию для передачи больших объёмов данных?
8. Как квантовая криптография противостоит квантовым вычислениям?
9. В каких странах уже внедрены реальные квантовые сети и проекты QKD?
10. Какие области в первую очередь нуждаются в защите с помощью квантовых методов?

Практическая часть

Задание 1. Анализ протокола BB84
Опишите пошагово работу протокола BB84. Нарисуйте схему обмена между Алисой и Бобом, указав все этапы — от генерации фотонов до обнаружения вмешательства.

Задание 2. Сравнение методов защиты
Сравните классическую криптографию (например, RSA или AES) и квантовую криптографию. Оформите сравнительный анализ в виде таблицы с параметрами: принцип действия, алгоритмическая основа, стойкость, уязвимости, применение.

Задание 3. Моделирование квантовой передачи ключа (на уровне логики)
Смоделируйте простейшую реализацию квантовой передачи ключа (например, на Python) с использованием псевдослучайных базисов и битов. Оцените, как изменяется финальный ключ при наличии/отсутствии вмешательства.

Задание 4. Краткий обзор реализованных проектов QKD
Исследуйте примеры реальных проектов: китайская спутниковая квантовая

сеть, Европейский проект OpenQKD, проект «Квантовая связь» в России. Опишите цели, инфраструктуру, достижения, особенности.

Задание 5. Разработка концепции внедрения QKD в защищённую систему
Представьте, что вы проектируете защищённый канал связи между двумя банковскими офисами. Опишите, какие компоненты квантовой криптографии вы бы использовали, какие задачи решаются, и какие вызовы вас ожидают.

Задание 6. Исследование влияния квантовых вычислений на криптографию
Ознакомьтесь с алгоритмами Шора и Гровера. Опишите, какие именно классические алгоритмы они делают уязвимыми. Сделайте вывод, почему возникает потребность в квантово-стойких системах защиты.

Ожидаемые результаты

В результате выполнения лабораторной работы студент:
– усвоит основы квантовой криптографии и протоколов квантовой передачи ключей;
– научится различать квантовые и классические подходы к защите информации;
– приобретёт практические навыки моделирования квантовой передачи на базовом уровне;
– получит представление о реальных проектах и перспективах квантовой защиты;
– сможет обосновать необходимость перехода к квантово-стойким технологиям в условиях угроз со стороны квантовых компьютеров.

Форма отчёта

– Титульный лист
– Теоретическая часть (краткое изложение основных понятий и принципов)
– Ответы на вопросы
– Выполнение практических заданий
– Выводы

Рекомендуемые источники и литература

1. В.В. Белоусов, «Квантовая криптография и квантовые вычисления»
2. Nielsen & Chuang, «Quantum Computation and Quantum Information»

3. Доклады ITU, ETSI, IEEE по теме квантовой защиты
4. Сайты: https://qkd.net, https://openqkd.eu, https://quantum.gov
5. Интерактивные симуляторы: Quantum Experience (IBM), QuTiP

Лабораторная работа 3

Разработка схемы защиты данных на основе блокчейн-технологий. Возможности применения блокчейна в системах информационной безопасности

Цель работы:
Изучить архитектуру и принципы функционирования блокчейн-технологий в контексте обеспечения информационной безопасности. Проанализировать особенности использования блокчейна для защиты данных, а также реализовать модель безопасной системы хранения и обмена информацией на его основе.

Теоретическая часть

1. Актуальность блокчейн-технологий в ИБ
С ростом объёмов данных, потребности в прозрачности и доверии в распределённых системах, блокчейн приобрёл статус одной из ключевых технологий. Он обеспечивает децентрализованное хранение информации, защиту от подделок, отказоустойчивость и криптографическую целостность записей. Блокчейн находит применение в финансовых технологиях, документообороте, здравоохранении, IoT и, конечно, в системах информационной безопасности.

2. Основные принципы технологии блокчейн
Блокчейн представляет собой связный список блоков, где каждый блок содержит данные, временную метку и криптографическую хеш-ссылку на предыдущий блок. Основные характеристики:
– Децентрализация (отсутствие единого узла управления)
– Невозможность изменения информации задним числом
– Криптографическая защищённость
– Использование консенсусных алгоритмов для валидации блоков (PoW, PoS, BFT и др.)

3. Элементы архитектуры
– Узлы (nodes): участники сети
– Смарт-контракты: автоматизированные условия исполнения соглашений
– Хеш-функции: защита целостности данных

– Цепочка блоков: защищённая история изменений
– Алгоритм консенсуса: подтверждение достоверности новой информации

4. Возможности применения в системах ИБ
– Контроль целостности данных и журналов событий
– Защита от фальсификации документов
– Доверенные цепочки поставок и происхождения (supply chain)
– Хранение цифровых идентификаторов и аутентификация
– Безопасное распределение ключей
– Управление правами доступа в децентрализованных системах

5. Преимущества и вызовы
Преимущества:
– Устойчивость к подделке данных
– Прозрачность
– Аудитируемость
– Отказоустойчивость
Ограничения:
– Производительность (особенно в публичных блокчейнах)
– Проблемы масштабирования
– Правовые и нормативные аспекты
– Необратимость транзакций

Вопросы для обсуждения

1. Какие ключевые преимущества делает блокчейн применимым в информационной безопасности?
2. В чём отличие публичного и частного блокчейна? Какие из них применимы в ИБ?
3. Как работает алгоритм консенсуса? Почему он важен?
4. Какие криптографические механизмы используются в блокчейне?
5. Как блокчейн может использоваться для защиты журналов событий (логов)?
6. Что такое смарт-контракт и как он может обеспечить безопасность?
7. Какие угрозы могут возникать при использовании блокчейна?
8. Возможно ли использовать блокчейн для контроля доступа к данным? Как?
9. Какие примеры реального применения блокчейна в ИБ вы знаете?
10. Как можно обеспечить конфиденциальность в открытой блокчейн-системе?

Практическая часть

Задание 1. Анализ блокчейн-сценариев в ИБ
Опишите минимум три возможных сценария использования блокчейна для защиты информации (например, защита аудита, управление доступом, система контроля версий). Укажите, какие технологии, алгоритмы и архитектурные подходы вы бы использовали.

Задание 2. Разработка простой модели хранения данных на блокчейне
На языке Python (или JavaScript с использованием библиотеки Web3, либо в среде Ganache + Solidity) разработайте простую модель цепочки блоков:
– Структура блока
– Добавление нового блока
– Проверка целостности цепочки
– Хеширование содержимого блока
Реализуйте имитацию добавления данных о транзакциях или событиях системы.

Задание 3. Смарт-контракт для авторизации пользователя
Используя язык Solidity, напишите смарт-контракт, обеспечивающий регистрацию и аутентификацию пользователей по их адресам. Добавьте базовые функции управления ролями (например, администратор, пользователь).

Задание 4. Анализ уязвимостей в блокчейн-средах
Изучите примеры известных инцидентов в блокчейн-системах (например, атака DAO, ошибки в смарт-контрактах). Опишите, какие уроки были извлечены и как можно предотвратить подобные ситуации в будущем.

Задание 5. Проектирование схемы защиты с блокчейн-ядром
Представьте, что вы проектируете защищённую систему электронного документооборота. Разработайте архитектурную схему:
– Где и как хранится информация
– Как используется блокчейн для верификации и целостности
– Какие механизмы защиты реализованы на каждом этапе

Оформите в виде схемы (можно использовать draw.io, PlantUML или графику от руки с пояснением).

Ожидаемые результаты

В результате выполнения лабораторной работы студент:
– Освоит принципы работы блокчейна и его архитектуру
– Сможет применить блокчейн в контексте защиты информации
– Получит практические навыки работы с моделью блокчейна и смарт-

контрактами
– Изучит реальные сценарии использования и проанализирует риски
– Будет способен спроектировать схему защиты с использованием децентрализованных подходов

Форма отчёта

– Титульный лист
– Теоретическая часть
– Ответы на вопросы
– Результаты практических заданий (с кодом, скриншотами и пояснениями)
– Разработанная схема или архитектурная модель
– Выводы

Рекомендуемые источники и литература

1. Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System"
2. Антонопулос А. "Мастеринг биткойн"
3. Курс IBM: Blockchain Essentials (Coursera, edX)
4. Solidity documentation: https://docs.soliditylang.org
5. OpenZeppelin smart contract library
6. Ganache, Truffle Suite – инструменты для локального тестирования блокчейн-сред

Лабораторная работа 4

Исследование применения ИИ в системах обнаружения атак. Роль машинного обучения в автоматизации киберзащиты

Цель работы:
Изучить принципы применения искусственного интеллекта (ИИ) и машинного обучения (МО) в задачах кибербезопасности. Ознакомиться с архитектурой систем обнаружения атак на основе ИИ, провести анализ эффективности различных методов обучения для распознавания вредоносной активности и разработать прототип модели обнаружения вторжений.

Теоретическая часть

1. Актуальность ИИ в кибербезопасности
С развитием цифровых технологий объёмы данных, поступающих в системы мониторинга, значительно увеличиваются. Традиционные сигнатурные

методы становятся менее эффективными против сложных, новых или целевых атак. В этой связи ИИ и машинное обучение открывают новые возможности автоматизации, адаптивности и интеллектуального анализа поведения.

2. Принципы машинного обучения в киберзащите
Машинное обучение предполагает выявление закономерностей в данных без явного программирования логики. Для задач кибербезопасности чаще всего применяются:
– Классификация (например, нормальное поведение vs атака)
– Кластеризация (выделение аномалий)
– Обнаружение выбросов (outlier detection)
– Последовательный анализ событий (с помощью RNN, LSTM)
– Глубокое обучение (нейронные сети, автоэнкодеры и др.)

3. Архитектура систем на основе ИИ
Типичная система обнаружения атак с ИИ-моделью включает:
– Модуль сбора и предобработки данных
– Этап извлечения признаков
– Обучающую выборку и метки классов
– Модель машинного обучения (SVM, Random Forest, XGBoost, нейросети и др.)
– Модуль принятия решений и оповещений
– Механизмы переобучения и адаптации

4. Источники данных для обучения
– Сетевые пакеты (pcap-файлы, NetFlow)
– Журналы событий (лог-файлы)
– Датасеты вторжений (например, CIC-IDS2017, KDD99, UNSW-NB15)
– Телеметрия от конечных устройств
– Профили поведения пользователей (UEBA)

5. Преимущества ИИ-подходов
– Автоматизация анализа больших объёмов данных
– Обнаружение неизвестных угроз (zero-day)
– Гибкость и адаптивность к изменениям в поведении атакующих
– Обучение в реальном времени (on-line learning)

6. Ограничения и вызовы
– Необходимость валидации данных и защита от "отравления" (data poisoning)
– Высокие требования к качеству и объёму обучающей выборки
– Возможность ложных срабатываний
– Интерпретируемость решений модели (explainable AI)

Вопросы для обсуждения

1. Почему традиционные методы обнаружения атак становятся менее эффективными?
2. В чём разница между сигнатурным методом и методом, основанным на ИИ?
3. Какие задачи кибербезопасности можно автоматизировать с помощью ИИ?
4. Какие алгоритмы машинного обучения чаще всего применяются для обнаружения атак?
5. Что такое переобучение (overfitting) и как его избежать?
6. Как обеспечивается защищённость моделей ИИ от внешнего вмешательства?
7. Какие существуют открытые датасеты для обучения моделей обнаружения атак?
8. Как оценить качество работы модели (точность, полнота, F1-score)?
9. Что представляет собой процесс извлечения признаков?
10. Какова роль глубинных нейронных сетей в задачах ИБ?

Практическая часть

Задание 1. Обзор инструментов ИИ в кибербезопасности
Составьте краткий обзор (0.5–1 стр.) существующих платформ и решений, использующих ИИ для защиты от киберугроз (например, Darktrace, Vectra AI, Cisco Secure Network Analytics, Elastic ML). Отразите их особенности, области применения и алгоритмы, если известно.

Задание 2. Работа с датасетом CIC-IDS2017
Загрузите и изучите датасет CIC-IDS2017 (или аналогичный). Проведите предварительную обработку:
– Удалите пропущенные значения
– Проведите нормализацию или стандартизацию
– Разделите выборку на обучающую и тестовую
– Выделите основные признаки (features)
Оформите результаты в виде отчёта с графиками и таблицами.

Задание 3. Обучение модели обнаружения атак
На основе обработанных данных обучите модель классификации, используя один из алгоритмов:
– Logistic Regression
– Decision Tree
– Random Forest
– SVM
– Нейронная сеть (по желанию)

Оцените качество модели с помощью метрик: accuracy, precision, recall, F1-score.
Отразите полученные результаты в виде таблицы.

Задание 4. Сравнительный анализ моделей
Обучите минимум две разные модели и сравните их результаты.
Сделайте вывод: какая модель подходит лучше для задач обнаружения атак в данной выборке и почему.

Задание 5. Имитация аномального поведения
Сгенерируйте искусственную аномалию в наборе данных (например, высокую частоту запросов от одного источника) и проверьте, может ли модель её обнаружить.
Опишите поведение модели при столкновении с незнакомым типом атаки.

Ожидаемые результаты

После выполнения лабораторной работы студент:
– Поймёт архитектуру систем ИИ для обнаружения атак
– Получит практические навыки работы с реальными данными в кибербезопасности
– Сможет обучать и анализировать модели машинного обучения
– Изучит основные алгоритмы классификации в контексте ИБ
– Сформирует навыки критической оценки качества моделей и их применения

Форма отчёта

– Теоретическая часть
– Ответы на вопросы
– Обзор инструментов
– Результаты анализа датасета
– Код обучения модели (фрагменты, скриншоты, Jupyter Notebook по желанию)
– Таблицы и графики с результатами
– Выводы

Рекомендуемые инструменты

– Jupyter Notebook
– Scikit-learn
– Pandas, Matplotlib, Seaborn

– TensorFlow или PyTorch (по желанию)
– CIC-IDS2017 dataset (https://www.unb.ca/cic/datasets/ids-2017.html)

Лабораторная работа 5.

Практика построения системы Zero Trust в корпоративной среде. Концепция полного недоверия как основа новой архитектуры безопасности

Цель работы:
Изучить архитектуру и принципы концепции Zero Trust, проанализировать ключевые компоненты модели полного недоверия, исследовать практики внедрения Zero Trust в корпоративной инфраструктуре, а также смоделировать базовую архитектуру Zero Trust-системы с учётом аутентификации, контроля доступа и сегментации сети.

Теоретическая часть

1. Сущность модели Zero Trust
Концепция Zero Trust (нулевого доверия) базируется на принципе: «никому не доверяй, всегда проверяй». В отличие от традиционной модели периметровой безопасности, где защита фокусируется на границе сети, Zero Trust предполагает, что ни один пользователь, устройство или приложение не заслуживают доверия по умолчанию — вне зависимости от того, находятся они внутри корпоративной сети или за её пределами.

2. Основные принципы Zero Trust:
– Проверка каждого запроса независимо от местоположения источника
– Минимальные привилегии: доступ только к необходимым ресурсам
– Многофакторная аутентификация (MFA)
– Сегментация и микросегментация сетей
– Контроль поведения и непрерывный мониторинг
– Анализ рисков в реальном времени

3. Компоненты архитектуры Zero Trust:
– Идентификация и управление доступом (Identity and Access Management, IAM)
– Политики управления доступом на основе атрибутов (ABAC)
– Контроль устройств (device health, compliance)
– Прокси и шлюзы для доступа к приложениям (например, ZTNA)
– Журналы аудита и аналитика поведения
– Политики управления данными и их шифрование

4. Внедрение Zero Trust: этапы
– Инвентаризация ресурсов и пользователей
– Создание политики сегментации
– Настройка систем IAM и MFA
– Обеспечение видимости трафика
– Внедрение динамического контроля доступа
– Постоянный аудит и пересмотр политик

5. Технологии и инструменты:
– Microsoft Entra (ex-Azure AD), Okta, Duo Security
– Google BeyondCorp, Zscaler
– Cisco Zero Trust, Palo Alto Prisma
– Open Policy Agent (OPA), HashiCorp Vault
– SIEM, UEBA, XDR-решения

Вопросы для обсуждения

1. Чем Zero Trust отличается от классической модели безопасности?
2. Какие уязвимости решаются при переходе к архитектуре полного недоверия?
3. Что такое микросегментация, и как она реализуется?
4. Почему критично контролировать устройства в модели Zero Trust?
5. Какие сложности могут возникнуть при реализации Zero Trust в крупной компании?
6. Что такое ZTNA, и в чём его отличие от VPN?
7. Какие метрики и логи необходимо собирать в архитектуре Zero Trust?
8. Как реализовать принцип минимальных привилегий на уровне приложений?
9. Почему модель Zero Trust особенно актуальна в условиях удалённой работы?
10. Какие шаги следует предпринять для первичного перехода к Zero Trust?

Практическая часть

Задание 1. Анализ текущих подходов к безопасности в организации
Опишите традиционную архитектуру безопасности компании (реальной или гипотетической). Укажите возможные риски, вызванные избыточным доверием внутри сети. Предложите, какие элементы требуют пересмотра при переходе к Zero Trust.

Задание 2. Построение модели Zero Trust
Разработайте логическую схему внедрения Zero Trust в корпоративную сеть.

Включите в модель:
– политики доступа на основе ролей или атрибутов
– механизм проверки подлинности и MFA
– методы контроля устройств
– сценарии микросегментации
– элементы логирования и мониторинга
Схему можно выполнить в любом графическом редакторе или на бумаге (и приложить фото/скан).

Задание 3. Конфигурация среды с базовыми элементами Zero Trust (эмуляция)
Используя платформу (например, виртуальную машину с Ubuntu Server + OpenLDAP + WireGuard + Fail2Ban), реализуйте эмуляцию простейших компонентов Zero Trust:
– Ограничьте SSH-доступ только проверенным IP
– Включите двухфакторную аутентификацию (например, Google Authenticator)
– Установите контроль неактивных сессий
– Настройте firewall по принципу deny-all
Сделайте скриншоты команд и настроек, поясните каждый шаг.

Задание 4. Анализ трафика и мониторинг поведения
Установите и настройте простую систему мониторинга поведения и логов (например, Wazuh или Suricata).
Проведите тестовые подключения и проверьте, как система фиксирует аномальные действия.
Опишите в отчёте логи и результаты анализа.

Задание 5. Кейс: внедрение Zero Trust в распределённой компании
Представьте, что вы ИБ-специалист в компании с удалёнными офисами и гибридной инфраструктурой. Опишите в свободной форме (1–2 страницы), какие шаги вы предпримете для реализации Zero Trust:
– какие политики будут внедрены
– какие решения выбраны (например, ZTNA вместо VPN)
– как будет контролироваться доступ к чувствительным данным
– как обеспечивается отказоустойчивость и адаптация к масштабированию

Ожидаемые результаты

По завершении лабораторной работы студент:
– Освоит теоретические основы архитектуры Zero Trust
– Поймёт подходы к минимизации доверия внутри ИТ-инфраструктуры
– Получит практические навыки моделирования Zero Trust-системы
– Ознакомится с инструментами контроля, аутентификации и сегментации

– Сможет формировать предложения по переходу организации к Zero Trust-архитектуре

Форма отчёта

– Теоретическая часть
– Ответы на вопросы
– Схема архитектуры
– Скриншоты конфигурации
– Анализ логов
– Кейсовое описание внедрения
– Выводы

Лабораторная работа 6.

Моделирование защищённого обмена в среде интернета вещей (IoT). Проблемы и решения безопасности в IoT-системах

Цель работы:
Изучить особенности архитектуры IoT-среды, рассмотреть основные угрозы и уязвимости, возникающие при взаимодействии IoT-устройств, а также смоделировать базовую схему защищённого обмена данными с применением методов аутентификации, шифрования и контроля доступа в контексте IoT.

Теоретическая часть

1. Особенности IoT-среды

Интернет вещей (IoT) — это система, включающая в себя физические устройства, оснащённые датчиками, программным обеспечением и сетевыми технологиями, позволяющими обмениваться данными. Основной особенностью является ограниченность ресурсов: низкая вычислительная мощность, ограниченная память и энергоэффективность.

2. Угрозы безопасности в IoT

IoT-среда подвержена множеству угроз, включая:
– Подделку идентичности устройства
– Перехват и подмену данных
– DDoS-атаки (включая ботнеты, как Mirai)
– Уязвимости прошивок
– Отсутствие или слабая реализация шифрования
– Отсутствие регулярного обновления ПО
– Недостаточный контроль доступа

3. Требования к безопасности IoT-систем:
– Надёжная аутентификация устройств
– Шифрование данных при передаче
– Управление ключами
– Контроль целостности прошивок
– Сегментация сети
– Лёгкие протоколы безопасности (например, DTLS, CoAP, MQTT с TLS)

4. Модели защищённого взаимодействия:
В контексте IoT взаимодействие часто происходит между:
– Устройствами (M2M)
– Устройствами и шлюзами (Device-to-Gateway)
– Устройствами и облачными сервисами (Device-to-Cloud)
– Устройствами и пользователями (Device-to-Human)

Для всех типов требуется реализация доверенной передачи данных, надёжной идентификации и защиты от атак «человек посередине» (MitM).

5. Технологии и инструменты:
– Протокол MQTT с TLS
– Протокол CoAP с DTLS
– IoT-платформы: ThingsBoard, AWS IoT, Azure IoT Hub
– Протоколы авторизации: OAuth 2.0, X.509 сертификаты
– Аппаратные модули безопасности: TPM, Secure Element
– Модели lightweight-криптографии: ECC, ChaCha20, Curve25519

Вопросы для обсуждения

1. Какие особенности безопасности отличают IoT-среду от традиционных IT-систем?
2. Каковы наиболее критичные уязвимости IoT-устройств?
3. В чём заключаются сложности реализации криптографии в IoT?
4. Как обеспечить надёжную аутентификацию устройств с ограниченными ресурсами?
5. Чем отличается CoAP от HTTP в контексте безопасности?
6. Какие модели взаимодействия характерны для IoT?
7. Какие угрозы в первую очередь возникают при использовании публичных сетей?
8. Какую роль играет облако в обеспечении безопасности IoT?
9. Что такое TPM и как он может применяться в IoT?
10. В каких случаях применима лёгкая криптография и каковы её примеры?

Практическая часть

Задание 1. Анализ типичной IoT-системы и её угроз
Опишите архитектуру условной IoT-системы (например, "умный дом", промышленный мониторинг или агроплатформа). Выделите ключевые компоненты (датчики, шлюзы, облако) и опишите возможные векторы атак.

Задание 2. Проектирование схемы защищённого взаимодействия
Постройте схему защищённого обмена данными между IoT-устройством, шлюзом и облачным сервисом. Укажите, на каком уровне применяются:
– Шифрование (например, TLS, DTLS)
– Аутентификация (пароли, сертификаты, токены)
– Управление ключами
– Защита от MitM и Replay-атак

Задание 3. Эмуляция защищённого взаимодействия (на уровне MQTT)
Используйте платформу (например, Mosquitto + Python-клиент paho-mqtt) для настройки защищённого взаимодействия между "виртуальным" устройством и брокером.
– Настройте TLS
– Реализуйте простую проверку клиентского сертификата
– Проведите обмен сообщениями и проанализируйте их в снифферe (например, Wireshark)
– Зафиксируйте конфигурацию и поясните шаги

Задание 4. Разработка политики безопасности для IoT-сети
Сформулируйте документ из 7–10 пунктов, описывающий политику безопасности для IoT-системы предприятия:
– порядок обновления прошивок
– политика смены ключей
– контроль устройств
– мониторинг активности
– реагирование на инциденты
– контроль доступа по ролям

Задание 5. Исследование криптографических алгоритмов для IoT
Сравните алгоритмы AES-256 и ChaCha20, RSA и ECC по параметрам: производительность, энергопотребление, надёжность. Выводы оформите в таблицу.

Ожидаемые результаты

Студент должен:
– Понять ключевые угрозы и уязвимости IoT-сред
– Ознакомиться с протоколами защищённого обмена

– Сконструировать базовую схему безопасного взаимодействия устройств
– Получить практические навыки настройки безопасных IoT-соединений
– Сформировать основы политик безопасности для систем IoT

Форма отчёта

– Теоретическая часть
– Ответы на вопросы
– Схема взаимодействия
– Скриншоты настроек и логов
– Таблица сравнения алгоритмов
– Политика безопасности
– Выводы

Лабораторная работа 7.

Применение гомоморфного шифрования для обработки зашифрованных данных. Перспективы и ограничения криптографии без расшифровки

Цель работы:
Изучить теоретические основы гомоморфного шифрования, его применимость к безопасной обработке данных без их предварительной расшифровки. Проанализировать возможности, ограничения и перспективы развития гомоморфных схем, а также реализовать простейшее моделирование гомоморфных операций.

Теоретическая часть

1. Основы гомоморфного шифрования

Гомоморфное шифрование — это метод криптографии, который позволяет выполнять вычисления над зашифрованными данными, не расшифровывая их. Результат таких операций после расшифровки будет идентичен результату, полученному над исходными открытыми данными.

2. Виды гомоморфного шифрования

– Частично гомоморфное (PHE): поддерживает только одну операцию (сложение или умножение), примеры: RSA, ElGamal, Paillier
– Ограниченно гомоморфное (SHE): поддерживает ограниченное количество операций и уровней
– Полностью гомоморфное (FHE): позволяет выполнять произвольные

арифметические операции и логические схемы над зашифрованными данными

3. Применение гомоморфного шифрования
– Облачные вычисления: безопасная обработка пользовательских данных на внешних серверах
– Медицинские и финансовые системы: конфиденциальный анализ чувствительной информации
– Защищённый сбор статистики
– Безопасная биометрическая аутентификация

4. Преимущества и ограничения
Преимущества:
– Обеспечение конфиденциальности на всех этапах обработки
– Минимизация рисков утечки при передаче и хранении
Ограничения:
– Высокие вычислительные затраты
– Значительное увеличение размера данных
– Сложность реализации и интеграции
– Ограниченное количество библиотек и платформ

5. Современные библиотеки и платформы
– Microsoft SEAL
– HElib (IBM)
– Palisade
– TenSEAL (для ML)
– PySEAL (обёртка для Python)

Вопросы для обсуждения

1. В чём заключается принцип гомоморфного шифрования?
2. Какие отличия между PHE, SHE и FHE?
3. Какие операции можно выполнять над зашифрованными данными в различных моделях?
4. Где гомоморфное шифрование применимо в реальных задачах?
5. Каковы основные сложности при использовании FHE в промышленности?
6. Какие существуют библиотеки для работы с гомоморфным шифрованием?
7. Как гомоморфия влияет на производительность вычислений?
8. Почему гомоморфное шифрование может быть предпочтительным для облачной обработки данных?
9. Какие угрозы устраняет гомоморфное шифрование?
10. Какие перспективы развития этой технологии в ближайшем будущем?

Практическая часть

Задание 1. Сравнение схем гомоморфного шифрования
Подготовьте таблицу, в которой сравните три схемы (Paillier, ElGamal, BGV) по критериям: тип поддерживаемой операции, сложность, устойчивость, применимость.

Задание 2. Реализация примера гомоморфных операций
С использованием библиотеки Microsoft SEAL или PySEAL:
– Зашифруйте два целых числа
– Выполните над ними операцию (сложение или умножение)
– Расшифруйте результат и проверьте его корректность
Оформите скрипт, укажите параметры шифрования и кратко объясните каждый шаг

Задание 3. Моделирование защищённого облачного вычисления
Опишите гипотетическую задачу (например, расчёт среднего значения зарплаты на сервере без раскрытия значений). Определите:
– Какие данные подлежат шифрованию
– Какие операции должны быть выполнены
– Как обеспечивается сохранность данных при вычислениях
– Потенциальные сложности при реализации

Задание 4. Анализ эффективности FHE-схем
Проведите исследование (на основе документации или эксперимента), как изменяется:
– Время выполнения операций
– Объём зашифрованных данных
при использовании различных параметров схемы (битность, количество уровней, тип операций). Представьте результат в виде диаграммы или таблицы.

Задание 5. Исследование перспектив и ограничений
Подготовьте короткий доклад (0.5–1 стр.) по теме: «Гомоморфное шифрование в защите данных: потенциал и барьеры внедрения». Укажите отрасли, где применение FHE наиболее актуально, и какие преграды стоят на пути его массового распространения.

Ожидаемые результаты

Студент должен:
– Освоить базовые понятия и виды гомоморфного шифрования
– Получить практический опыт в шифровании и обработке данных без их

раскрытия
– Понять применимость гомоморфии в облачных и распределённых системах
– Провести аналитическую оценку производительности и ограничений методов
– Научиться обосновывать выбор конкретных криптографических подходов

Форма отчёта

– Ответы на теоретические вопросы
– Скрипт или псевдокод шифрования и обработки данных
– Таблицы сравнения схем
– Диаграммы или таблицы по производительности
– Схема или описание облачной задачи
– Доклад по перспективам
– Выводы

Лабораторная работа 8

Анализ методов биометрической аутентификации будущего. Новые направления в биометрии: поведенческие и нейронные признаки

Цель работы:
Изучить современные и перспективные подходы к биометрической аутентификации. Ознакомиться с новыми направлениями в биометрии, такими как поведенческие и нейронные признаки, их характеристиками, преимуществами и рисками. Проанализировать применимость данных методов в реальных системах информационной безопасности.

Теоретическая часть

1. Эволюция биометрической аутентификации
Традиционные биометрические методы включают отпечатки пальцев, распознавание лица, радужки глаза, голосовую биометрию. С развитием технологий и появлением новых угроз на первый план выходят поведенческие и нейроповеденческие биометрические признаки, которые труднее подделать и которые сложнее эксплуатировать.

2. Поведенческая биометрия
Включает в себя распознавание личности по динамике набора текста

(keystroke dynamics), особенностям походки, почерку, движениям мыши, стилю взаимодействия с устройствами.
Такие признаки зависят от множества параметров, включая психологическое и физическое состояние человека, и являются уникальными даже в микродеталях.

3. Нейронные и когнитивные признаки
Когнитивная биометрия опирается на особенности реакции мозга, фиксируемые через ЭЭГ-сигналы, зрительные стимулы, ответы на определённые задачи. Эти признаки глубже физиологических и поведенческих, так как связаны с внутренней нейронной активностью. Появление коммерчески доступных ЭЭГ-гарнитур открыло возможность практического применения этих подходов.

4. Преимущества новых методов
– Сложность подделки
– Высокая устойчивость к взлому
– Постоянное обновление шаблона (динамика)
– Возможность бесконтактной или непрерывной аутентификации

5. Ограничения и риски
– Высокие требования к оборудованию
– Неустойчивость к шумам и изменениям состояния пользователя
– Вопросы приватности и медицинской этики (особенно в случае нейропоказателей)
– Сложности стандартизации и нормативного регулирования

Вопросы для обсуждения

1. Каковы ключевые отличия между физиологической, поведенческой и когнитивной биометрией?
2. В чём заключается принцип работы динамики набора текста?
3. Какие методы могут использоваться для распознавания по стилю мышиного движения?
4. Какие данные используются в когнитивной биометрии?
5. Какие преимущества дают поведенческие признаки по сравнению с традиционными?
6. Какие вызовы стоят перед применением нейробиометрии?
7. Какие технологии и устройства применяются для регистрации нейросигналов?
8. Какие есть риски злоупотреблений в контексте поведенческой и когнитивной биометрии?
9. Может ли поведенческая биометрия применяться в непрерывной аутентификации?

10. В каких отраслях наиболее вероятно появление новых биометрических систем?

Практическая часть

Задание 1. Обзор современных решений
Проведите анализ существующих продуктов и стартапов, применяющих поведенческую или когнитивную биометрию. Составьте таблицу: название системы, вид биометрии, область применения, уровень точности, плюсы и минусы.

Задание 2. Моделирование поведенческой аутентификации
Используя Python (или другой язык), реализуйте простую модель распознавания пользователя по ритму набора текста.
– Соберите данные нескольких пользователей
– Преобразуйте их в векторы (время между нажатиями, длительность удержания)
– Используйте алгоритм классификации (например, kNN или Random Forest)
– Проанализируйте точность

Задание 3. Исследование устойчивости поведенческой биометрии
Смоделируйте изменение поведения пользователя (например, изменение скорости набора при усталости) и проверьте, как меняется точность аутентификации.
Оформите вывод: как можно повысить устойчивость модели?

Задание 4. Когнитивная биометрия (теоретическое моделирование)
Изучите алгоритмы распознавания личности по ЭЭГ-сигналам.
Опишите:
– Какие особенности сигнала учитываются
– Какие задачи дают пользователю
– Какие методы машинного обучения используются
– Какие проблемы возникают при регистрации и интерпретации

Задание 5. Анализ рисков
Подготовьте краткий аналитический доклад (0.5–1 стр.) на тему: «Поведенческая и нейробиометрия: риски приватности, этики и прав человека».
Отразите потенциальные сценарии злоупотреблений и возможные способы их предотвращения.

Ожидаемые результаты

Студент должен:
– Знать и уметь различать современные виды биометрической аутентификации
– Понимать перспективы развития поведенческих и нейронных методов
– Уметь реализовывать простейшие модели анализа поведенческих признаков
– Анализировать потенциальные угрозы и сложности внедрения
– Владеть подходами к этической и технической оценке новых технологий

Форма отчёта

– Ответы на теоретические вопросы
– Скрипт или описание модели поведенческой биометрии
– Таблица сравнения биометрических решений
– Доклад по когнитивной биометрии
– Анализ рисков и краткий вывод

Лабораторная работа 9.

Проектирование системы защиты облачного хранилища. Тенденции развития облачных вычислений и связанных с ними угроз

Цель работы:
Ознакомиться с архитектурой облачных хранилищ, выявить ключевые угрозы информационной безопасности в условиях использования облачных технологий, изучить современные подходы и методы проектирования комплексной системы защиты данных в облаке.

Теоретическая часть

1. Современное состояние и развитие облачных вычислений

Облачные технологии стали неотъемлемой частью информационной инфраструктуры бизнеса, государственного сектора и частных пользователей. Они обеспечивают масштабируемость, отказоустойчивость и экономию ресурсов, но вместе с этим порождают новые вызовы для обеспечения конфиденциальности, целостности и доступности информации.

2. Типы облачных сервисов и моделей развертывания

Облачные вычисления реализуются в различных форматах: IaaS (инфраструктура как услуга), PaaS (платформа как услуга), SaaS

(программное обеспечение как услуга). Также различают модели развертывания: публичное, частное, гибридное и мультиоблако. Каждая модель предъявляет свои требования к безопасности и определяет набор угроз.

3. Актуальные угрозы облачных хранилищ
Среди основных угроз можно выделить:
– Несанкционированный доступ к данным
– Атаки на гипервизор и межмашинные каналы
– Утечка данных при передаче
– Нарушения прав доступа и слабая аутентификация
– Использование облака злоумышленниками для распространения вредоносного ПО
– Потеря контроля над данными при передаче полномочий облачному провайдеру

4. Основные принципы проектирования защищённого облачного хранилища
– Шифрование данных на всех этапах: в покое, в передаче, в обработке
– Надёжная аутентификация и управление доступом
– Использование сегментированной архитектуры (Zero Trust)
– Мониторинг событий и обнаружение аномалий
– Внедрение политики резервного копирования и восстановления
– Прозрачность взаимодействия с провайдером (SLA, стандарты)
– Аудит и регулярное тестирование на уязвимости

5. Тенденции и технологии защиты облачных сред
Современные средства защиты включают в себя:
– Шифрование с разделением ключей (Bring Your Own Key, BYOK)
– Контейнеризация и микросервисная архитектура
– Использование аппаратных модулей безопасности (HSM)
– Виртуальные частные облака (VPC)
– Облачные межсетевые экраны и системы предотвращения вторжений
– Поведенческий анализ пользователей (UEBA)
– Автоматизация реагирования (SOAR)

Вопросы для обсуждения

1. Какие преимущества и риски несут облачные хранилища данных?
2. Чем отличается защита публичного и частного облака?
3. Как реализуется аутентификация пользователей в облачных системах?
4. Какие угрозы характерны для модели IaaS?
5. Какие методы применяются для защиты данных при передаче?

6. Что представляет собой концепция Zero Trust и как она реализуется в облаке?
7. Какие типы шифрования используются в облачных хранилищах?
8. Какие стандарты и нормативы применимы к облачной безопасности (например, ISO/IEC 27017)?
9. В чём преимущества использования BYOK?
10. Какие существуют способы контроля и аудита активности в облаке?

Практическая часть

Задание 1. Анализ угроз
Составьте таблицу, в которой отразите основные угрозы безопасности для облачного хранилища и соответствующие им меры защиты. Укажите тип угрозы, потенциальный ущерб и контрмеры.

Задание 2. Проектирование схемы защиты облака
Разработайте архитектурную схему защищённого облачного хранилища для корпоративной среды. Укажите точки контроля доступа, методы шифрования, компоненты безопасности (IDS, MFA, логирование и т.д.). Представьте схему в графическом виде и сопроводите пояснением.

Задание 3. Сравнительный анализ провайдеров
Изучите и сравните подходы к защите данных у трёх ведущих облачных провайдеров (например, AWS, Azure, Google Cloud). Подготовьте таблицу с критериями: аутентификация, шифрование, аудит, поддержка compliance, возможности BYOK и HSM.

Задание 4. Моделирование рисков
Представьте, что ваша компания передаёт хранилище конфиденциальных данных в публичное облако. Опишите потенциальные сценарии атак и предложите стратегию минимизации рисков. Оформите это в виде краткого отчёта (0.5–1 стр.).

Задание 5. Обоснование выбора архитектуры
На основе предыдущих заданий подготовьте текстовую пояснительную записку (1 стр.), в которой объясните выбранные меры защиты, их эффективность и актуальность в современных условиях.

Ожидаемые результаты

Студент должен:
– Понимать архитектуру и угрозы облачных вычислений
– Уметь классифицировать угрозы и сопоставлять им адекватные меры защиты

– Владеть базовыми принципами проектирования безопасных облачных хранилищ
– Анализировать подходы различных провайдеров к безопасности
– Разрабатывать собственные решения и аргументировать их эффективность

Форма отчёта

– Ответы на теоретические вопросы
– Таблица угроз и мер защиты
– Схема архитектуры и её описание
– Сравнение провайдеров
– Моделирование рисков
– Пояснительная записка