МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____/Бредихин А.В./

28.08.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Введение в специальность»

Специальность 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2025

Автор программы _____ А.Г. Остапенко

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ С.С. Куликов

Воронеж 2025

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Цель изучения дисциплины «Введение в специальность» – формирования целостной картины проблематики инфобезопасности, включая привитие будущим специалистам базовых знаний и умений в области анализа защищенности (уязвимостей) и обеспечения безопасности автоматизированных информационных систем и сетей.

1.2. Задачи освоения дисциплины

1. Освоение научно-методических основ кибер-безопасности, вовлечение будущих специалистов в проблематику сетевых войн и защиты современного (мультисетевого) пространства социотехнических систем.

2. Адекватное восприятие студентами сущности и важности проблемы обеспечения информационной безопасности личности, общества и государства через изучение основ и эффектов коммуникативного воздействия на психику индивида и социальной группы, включая привитие информационного иммунитета и снижение рисков вербовки студенческой молодежи в деструктивные культы и террористические организации.

3. Через ознакомление с цифровыми технологиями и методами социальной инженерии демонстрация преимуществ национальных демократических, культурных и духовно-нравственных ценностей и традиций и тем самым - снижение рисков участия студенческой молодежи в операциях кибер-преступных группировок и спровоцированных злоумышленниками противоправных акциях протеста (цветных революциях).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Введение в специальность» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б.1 учебного плана.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Введение в специальность» направлен на формирование следующих компетенций:

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-9.2 Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	**Знать**: архитектурные принципы построения средств защиты от несанкционированного доступа и компьютерных атак; требования к разработке защитных механизмов телекоммуникационных систем. **Уметь**: проектировать и реализовывать средства обнаружения и предотвращения атак, разрабатывать прототипы защитных систем, проводить их испытания. **Владеть**: навыками создания программно-аппаратных решений защиты сетей электросвязи (кроме специального назначения).
ПК-9.3 Способен моделировать защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации	**Знать**: принципы построения защищённых технических средств обработки информации; требования к программно-техническим средствам контроля доступа и защиты от несанкционированного воздействия. **Уметь**: разрабатывать защищённые устройства и комплексы, реализовывать механизмы доверенной загрузки и мандатного контроля доступа. **Владеть**: навыками проектирования аппаратных и программных компонентов систем защиты информации.
ПК-9.6 Способен разрабатывать предварительные проектные решения по защите информации	**Знать**: основные методы и подходы искусственного интеллекта и машинного обучения; области их применения в задачах обеспечения информационной безопасности. **Уметь**: разрабатывать и применять модели машинного обучения для обнаружения аномалий, анализа угроз и автоматизации процессов защиты. **Владеть**: навыками интеграции технологий искусственного интеллекта в системы мониторинга и реагирования на инциденты информационной безопасности.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Введение в специальность» составляет 5 зачетных единиц.

Распределение трудоемкости дисциплины по видам занятий

Очная форма обучения

Вид учебной работы	Всего часов	Семестры
		1
Аудиторные занятия (всего)	36	36
В том числе:		
Лекции	18	18
Практические занятия (ПЗ)	18	18
Лабораторные работы (ЛР)	0	0
Самостоятельная работа	108	108
Курсовой проект(работа) (есть, нет)	+	+
Контрольная работа (есть, нет)		нет
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)		зачет с оценкой
Общая трудоемкость час	144	144
зач. ед.	4	4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	Лаб. зан.	СРС	Все го, час
1	Учебный стандарт и план специальности в условиях цифровой трансформации и сетевой организации пространства	Значение автоматизированных систем для обеспечения информационной безопасности личности, общества и государства. Основные определения.	1	1	0	0	2
2	Проблема обеспечения безопасности автоматизированной информационной системы и сети	Цифровая трансформация и структура современной корпорации, модель корпоративной автоматизированной информационной системы, сети (АИС), оценка стоимости информационных ресурсов (ПКО). Модель угроз. Формирование требований к системе обеспечения информационной безопасности в автоматизированных системах корпорации. Организационно-технические мероприятия по защите информации при ее обработке, хранении и передаче в АИС.	2	2	0	0	4
3	Модели атакуемых автоматизированных сетей	Традиционная формализация описания сетей, взвешенные сети: матрицы и метрики, конфликтология взвешенных сетей, стратегические цели и тактические приемы сетевого противоборства, особенности сетевого терроризма.	2	2	0	0	4
	Эпидемические	Формализация описания сетевых структур и	1	1	0	0	2

4	модели автоматизированных сетей	процессов, компьютерные вирусы и эпидемии в информационно-телекоммуникационных сетях, вирусный контент и эпидемии в социальных сетях.					
5	Информационная безопасность и социальная инженерия в автоматизированных сетях	Основы информационно-психологического воздействия и управления социумом, контент как инструмент психологического воздействия и управления в информационном обществе, социальные сети как пространство распространения контентов влияния, информационно-психологические метрики контентов и интернет-ресурсов, управление информационно-психологическими рисками в целях обеспечения безопасности личности и социума.	2	2	0	0	4
6	Автоматизированные сети и деструктивный контент	Социальные сети как среда распространения контента, информационное обеспечение для описания процессов распространения контента в социальных сетях, методическое обеспечение для описания процессов распространения контента в социальных сетях, оценка и регулирование рисков распространения деструктивных контентов в социальных сетях.	2	2	0	0	4
7	Мониторинг безопасности автоматизированных сетей	Мониторинг и управление рисками социо-информационного пространства в целях обеспечения региональной и национальной безопасности, инструментальные и методические особенности контент-мониторинга социальных сетей, выявление деструктивных контентов в социальных сетях, риск-метрология для контент-мониторинга, мониторинг регионального интернет-пространства в контексте обеспечения социальной безопасности.	2	2	0	0	4
8	Перспективы цифровой трансформации и обеспечения безопасности автоматизированных сетей и систем на основе средств искусственного интеллекта	Базовые понятия информационной безопасности, методы защиты информации. Роль ИИ в кибербезопасности, оценка алгоритмов машинного обучения Обнаружение аномалий и атак в сетевом трафике. Применение МО для обнаружения сетевых атак и аномалий, межсетевые экраны и системы обнаружения вторжений Идентификация. Биометрия. Основы биометрии, виды аутентификации и задача от-бора признаков. Состязательные атаки на биометрические системы	2	2	0	0	4
9	Картографирование защищаемого кибер-сетевого пространства	Киберпространство как объект защиты и картографического исследования. Концептуальные основы картографии защищаемого киберпространства Информационная карта как основа картографирования защищаемого киберпространства. Вербальная модель процесса информационно-картографического исследования. Инструментальные основы картографии защищаемого киберпростраства. Реализация методологии картографирования защищаемого киберпространства в условиях информационного противоборства	2	2	0	0	4
10	Особенности обеспечения безопасности интернета вещей	Анализ безопасности технологий интернета вещей. Классификация угроз IoT. Примеры угроз для устройств интернета вещей в различных сферах	1	1	0	0	2
11	Результаты и перспективы реализации проекта «Безопасный интернет»		1	1	0	0	2
12	Риск-мониторинг Интернет-ресурса		0	0	0	108	108
		Итого	**18**	**18**		**108**	**144**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовой работы во 2 семестре.

Примерная тематика курсовой работы: «Риск-мониторинг интернет-ресурса»

Задачи, решаемые при выполнении курсового проекта:

- парсинг заданного ресурса на предмет выявления деструктивов, их классификация;
- измерение параметров деструктивов и формирование базы их данных;
- оценка рисков и выработка рекомендаций по противодействию деструктивам.

Курсовая работа включат в себя графическую часть и расчетно-пояснительную записку.

Учебным планом по дисциплине не предусмотрено выполнение контрольных работ.

Курсовая работа реализуется в рамках проекта «Безопасный интернет» (рег. № АААА-А18-118050700061-7)

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-9.2	**Знать**: архитектурные принципы построения средств защиты от несанкционированного доступа и компьютерных атак; требования к разработке защитных механизмов телекоммуникационных систем. **Уметь**: проектировать и реализовывать средства обнаружения и предотвращения атак, разрабатывать прототипы защитных систем, проводить их испытания. **Владеть**: навыками создания программно-аппаратных решений защиты сетей электросвязи (кроме специального назначения).	Знание архитектурных принципов построения средств защиты от несанкционированного доступа и компьютерных атак; требования к разработке защитных механизмов телекоммуникационных систем. Умение проектировать и реализовывать средства обнаружения и предотвращения атак, разрабатывать прототипы защитных систем, проводить их испытания. Владение навыками создания программно-аппаратных решений защиты сетей электросвязи (кроме специального назначения).	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-9.3	**Знать**: принципы построения защищённых технических средств обработки информации; требования к программно-техническим средствам контроля доступа и защиты от несанкционированного воздействия. **Уметь**: разрабатывать защищённые устройства и комплексы, реализовывать механизмы доверенной загрузки и мандатного контроля доступа. **Владеть**: навыками проектирования аппаратных и программных компонентов систем	Знание принципов построения защищённых технических средств обработки информации; требования к программно-техническим средствам контроля доступа и защиты от несанкционированного воздействия. Умение разрабатывать защищённые устройства и комплексы, реализовывать механизмы доверенной загрузки и мандатного контроля доступа. Владение навыками проектирования аппаратных и программных компонентов систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	защиты информации.	защиты информации.		
ПК-9.6	**Знать**: основные методы и подходы искусственного интеллекта и машинного обучения; области их применения в задачах обеспечения информационной безопасности. **Уметь**: разрабатывать и применять модели машинного обучения для обнаружения аномалий, анализа угроз и автоматизации процессов защиты. **Владеть**: навыками интеграции технологий искусственного интеллекта в системы мониторинга и реагирования на инциденты информационной безопасности.	Знание основных методов и подходов искусственного интеллекта и машинного обучения; области их применения в задачах обеспечения информационной безопасности. Уметь разрабатывать и применять модели машинного обучения для обнаружения аномалий, анализа угроз и автоматизации процессов защиты. Владеть навыками интеграции технологий искусственного интеллекта в системы мониторинга и реагирования на инциденты информационной безопасности.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются во 2 семестре:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл	Неудовл
ПК-9.2	Определяет основные угрозы безопасности информации и формализует модели нарушителя в автоматизированных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Разрабатывает модели угроз безопасности информации и модели нарушителя в автоматизированных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Разрабатывает аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
ПК-9.3	Осуществляет сбор и систематизация (анализ и оценка) сведений об угрозах НСД к сетям электросвязи	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Реализует проведение анализа структурных и функциональных схем, защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	Участвует в разработке программно-аппаратных средств защиты информации в компьютерных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень вопросов для подготовки к зачету

Краткое содержание

DOS И DDOS АТАКИ 1.3

1.1. Сущность DoS и DDos-атак4
Источник атаки
Сложность реализации
Методы атаки
Уровень опасности
5. Скрытность и обнаружение
1990-е: Рождение DDos-атак
2000-е: Первые мощные удары
2010-е: Хактивизм и новые инструменты
2020-е: Рекорды и новые подходы
2. Специфика реализации DoS и DDoS-атак
2.1. Сценарии реализации DoS-атак.
2.2. Сценарии реализации DDoS-атак.
Распределенные атаки
Специфика DDoS-атак
2.3. Инструменты и методы: популярные инструменты для проведения атак
Популярные инструменты DDoS-атак
Тенденции реализации DDoS-атак
3. Многообразие DoS и DDoS-атак
3.1. Протокольные атаки.
Примеры протокольных атак
Наносимые ущербы
Механизмы защиты
3.2. Атаки на уровне приложений
Сценарии атак на уровне приложений
Уязвимости приложений
Рекордные атаки
Рекомендации для бизнеса
3.3. Атаки на основе ботнетов
4. Последствия DoS и DDoS-атак
4.1. Экономические последствия: убытки для бизнеса и организаций
Финансовые убытки
Потеря репутации
Региональные особенности
4.2. Репутационные риски
Долгосрочные репутационные последствия
Стратегии минимизации репутационных рисков
4.3. Технические последствия
5. Методы защиты от DoS и DDoS-атак
5.1. Превентивные меры: как предотвратить атаки заранее.
5.2. Реагирование на атаки
Использование DDoS-защиты и WAF
Мониторинг и анализ трафика
Реагирование на атаки в реальном времени
Адаптация к новым типам угроз
Применение облачных решений для фильтрации трафика
5.3. Роль облачных решений и CDN в защите от атак.
Достоинства облачных решений для защиты от DDos-атак

Топ платформ защиты от DDoS-атак
6. Будущее DoS и DDos-атак
6.1. Тенденции в развитии атак
Приоритетные цели DDoS-атак
Причины изменения приоритетных целей
Влияние искусственного интеллекта на опасность DDoS-атак
6.2. Перспективы развития защиты

Контрольные вопросы

1. Введение (1.1 – 1.2)

1. В чем основная цель DoS и DDoS-атак?
2. Какое ключевое отличие DoS от DDoS?
3. Почему DDoS-атаки сложнее блокировать, чем DoS?
4. Какие методы чаще всего используются в DoS-атаках?
5. Назовите три основных типа DDoS-атак.
6. Почему DDoS-атаки считаются более опасными, чем DoS?
7. Какой год считается началом эры DDoS-атак?
8. Кто первым применил SYN Flood и против кого?
9. Какое событие в 1999 году показало опасность координированных DDoS-атак?
10. Какие известные платформы атаковал Mafiaboy в 2000-х?
11. Какой инцидент 2007 года считается первым актом кибервойны?
12. Какая атака в 2013 году достигла мощности 300 Гбит/с?
13. Какой ботнет в 2016 году атаковал Dyn DNS?
14. Какова была мощность атаки на Google в 2020 году?
15. Что такое HTTP/2 Rapid Reset и когда он появился?

2. Специфика реализации атак (2.1 – 2.3)

16. Как DoS-атаки перегружают ресурсы сервера?
17. Какие уязвимости чаще всего эксплуатируются в DoS-атаках?
18. Почему IoT-устройства стали популярной мишенью для атак?
19. Как злоумышленники используют открытые реестры в DoS-атаках?
20. Какие прогнозы даются о развитии DoS-атак?
21. Чем отличаются распределенные атаки (DDoS) от обычных DoS?
22. Что такое мультивекторная DDoS-атака?
23. Почему атаки на уровне приложений (L7) особенно опасны?
24. Какая отрасль чаще всего страдает от L7-атак?
25. Как долго может длиться самая продолжительная DDoS-атака?
26. Какие страны лидируют по числу источников DDoS-атак в 2024 году?
27. Что такое ботнет и как он используется в DDoS?
28. Какие инструменты из Kali Linux могут быть использованы для атак?
29. Чем LOIC отличается от HOIC?
30. Почему Mirai считается особенно опасным ботнетом?
31. На сколько процентов увеличилось число DDoS-атак в 2024 году?
32. Что такое «маломощные непрерывные атаки»?

3. Многообразие атак (3.1 – 3.3)

33. Как работает атака HTTP/2 Rapid Reset?
34. Какие уязвимости DNS используются в DDoS-атаках?
35. Как SYN Flood нарушает работу TCP-протокола?
36. Чем опасны атаки на основе IP-фрагментации?
37. Какие системы помогают защититься от протокольных атак?
38. Что такое HTTP-флуд и как он работает?
39. Как Slowloris истощает ресурсы сервера?
40. Что такое атака с использованием отражения (Reflection Attack)?
41. Как работает DNS Amplification?
42. Какие уязвимости приложений чаще всего эксплуатируются?
43. Какой процент финансовых потерь связан с атаками на веб-приложения?

44. Сколько запросов в секунду выдержала Google в 2023 году?
45. Какие меры защиты рекомендуются для бизнеса против L7-атак?
46. На сколько выросло число ботнетов с 2021 по 2023 год?
47. Какие устройства чаще всего входят в состав современных ботнетов?
48. Какие киберпреступления, кроме DDoS, совершают ботнеты?
49. Какие страны наиболее затронуты ботнетом Androxgh0st?
50. Какие уязвимости использует ботнет «gayfemboy»?

4. Последствия атак (4.1 – 4.3)

51. Какая отрасль чаще всего атакуется DDoS в 2023 году?
52. Какие финансовые потери несет бизнес из-за DDoS?
53. Почему репутационные риски так опасны для компаний?
54. Как DDoS-атаки влияют на телекоммуникационный сектор?
55. Какой регион наиболее подвержен DDoS-атакам на госструктуры?
56. Какие технические последствия вызывает DDoS на облачные сервисы?
57. Как атаки на энергетический сектор угрожают инфраструктуре?

5. Методы защиты (5.1 – 5.3)

58. Какие превентивные меры помогают защититься от DDoS?
59. Как WAF помогает в защите от атак на приложения?
60. Какие облачные решения лучше всего подходят для защиты от DDoS?

АТАКИ НА ОСНОВЕ IOT 1.3

1. Введение в IoT и его значимость
1.1. Определение IoT: описание концепции сети Интернет вещей и его компонентов.
1.2. Применение IoT в различных сферах: примеры использования в быту, промышленности и здравоохранении.
Применение IoT в здравоохранении
Применение IoT в промышленности
Применение IoT в быту
2. Уязвимости IoT-устройств
2.1. Проблемы безопасности: обзор распространенных уязвимостей в IoT-устройствах.
2.2. Недостатки протоколов связи: анализ протоколов, используемых в IoT, и их уязвимости.
1. MQTT (Message Queuing Telemetry Transport)
2. CoAP (Constrained Application Protocol)
3. HTTP (Hypertext Transfer Protocol)
4. Bluetooth
5. Zigbee
3. Типы атак на IoT-устройства
3.1. DDoS-атаки: описание Distributed Denial of Service атак и их влияние на IoT.
Примеры DDoS-атак на IoT-устройства
Влияние DDoS-атак на IoT и бизнес
3.2. Атаки на конфиденциальность: как злоумышленники могут получить доступ к личной информации пользователей.
3.3. Физические атаки: примеры атак, связанных с физическим доступом к устройствам.
4. Примеры реальных атак на IoT
4.1. Атака Mirai: анализ одной из самых известных DDoS-атак на IoT-устройства.
1. Механизм атаки Mirai
2. Последствия атак Mirai
3. Рекомендации по защите
4.2. Уязвимости в умных домах: примеры атак на системы умного дома и их последствия.5. Меры по защите IoT-устройств
5.1. Лучшие практики безопасности: рекомендации по обеспечению безопасности IoT-устройств.
Прогнозы и новые вызовы в области безопасности IoT в 2025 году
5.2. Роль производителей: ответственность производителей в обеспечении безопасности своих устройств.
6. Будущее безопасности IoT
6.1. Тенденции в развитии IoT: как меняется ландшафт IoT и его безопасность.

6.2. Перспективы технологий защиты: новые технологии и подходы к обеспечению безопасности IoT

Контрольные работы

1. Дайте определение концепции «Интернет вещей» (IoT).
2. Кто и когда впервые сформулировал концепцию IoT?
3. Назовите ключевые компоненты сети Интернет вещей.
4. Какую роль в IoT играют технологии идентификации, такие как RFID и QR-коды?
5. Что является основным предназначением датчиков (средств измерения) в IoT?
6. Почему переход на протокол IPv6 критически важен для развития IoT?
7. Приведите три примера применения IoT в быту.
8. Как IoT применяется в здравоохранении? Приведите конкретный пример.
9. Каковы преимущества использования IoT в промышленности на примере компаний Rolls Royce или John Deere?
10. Как умные термостаты и холодильники меняют повседневную жизнь пользователей?
11. Что, согласно блогу Brackish, является одной из самых распространенных уязвимостей IoT-устройств?
12. Почему небезопасные сетевые службы представляют угрозу для IoT?
13. К каким последствиям приводит отсутствие регулярных обновлений ПО для IoT-устройств?
14. Что такое «жестко закодированные пароли» и почему они опасны?
15. Какую динамику роста уязвимых IoT-устройств показал отчет компании Forescout за 2024 год?
16. Какие типы IoT-устройств являются наиболее уязвимыми согласно приведенной статистике?
17. Что такое «OWASP IoT Top Ten»?
18. Назовите три основные уязвимости из списка OWASP IoT Top Ten.
19. В чем заключается основная уязвимость протокола MQTT по умолчанию?
20. Как можно устранить недостаток шифрования в протоколе MQTT?
21. Какие проблемы безопасности характерны для протокола CoAP?
22. Почему HTTP считается небезопасным протоколом для использования в IoT?
23. Какие уязвимости Bluetooth были продемонстрированы на примере взлома плюшевого мишки и смарт-замков?
24. В чем заключаются основные недостатки безопасности протокола Zigbee?
25. Что такое DDoS-атака и какова ее основная цель?
26. Почему IoT-устройства стали популярной мишенью для создания ботнетов для DDoS-атак?
27. Приведите пример известного ботнета, использующего IoT-устройства для DDoS-атак.
28. Каковы были последствия атак ботнета Mirai согласно данным NETSCOUT?
29. Какие финансовые последствия для бизнеса могут иметь DDoS-атаки?
30. Как DDoS-атаки могут быть использованы в качестве отвлекающего маневра?
31. Каким образом слабые пароли на IoT-устройствах могут привести к атаке на конфиденциальность?
32. Что такое атака «человек посередине» (MitM) и как она угрожает конфиденциальности данных в IoT?
33. Как отсутствие шифрования передаваемых данных повышает риск для конфиденциальности пользователя?
34. Что такое физическая атака на IoT-устройство?
35. Приведите пример физической атаки, направленной на внутренние компоненты устройства.
36. Как злоумышленник может изменить поведение устройства через физический доступ?
37. Какие меры защиты рекомендуются для противодействия физическим атакам?
38. Какую роль в защите от физических атак играют такие компоненты, как TPM?
39. Что такое ботнет Mirai и в чем заключался его механизм действия?
40. Как развивались атаки на основе Mirai в 2024-2025 годах?
41. Какие уязвимости в IoT-устройствах эксплуатировали спин-оффы Mirai?
42. Какие рекомендации по защите от атак типа Mirai приведены в лекции?
43. Почему сегментация сети является эффективной мерой против распространения атак на IoT-устройствах?
44. Приведите пример атаки на систему умного дома с использованием уязвимости «человек посередине».

45. Какую опасность представляют собой программы-вымогатели (Ransomware) для владельцев умных домов?
46. Как взломанные IoT-устройства в умном доме могут быть использованы для создания ботнета?
47. Что такое уязвимость CVE-2024-12398 в устройствах Zyxel и чем она опасна?
48. Каковы основные рекомендации для пользователей по обеспечению безопасности IoT-устройств?
49. Почему регулярное обновление программного обеспечения критически важно для безопасности IoT?
50. Что подразумевается под «безопасным развертыванием оборудования»?
51. Какую роль в безопасности играет проведение регулярного аудита безопасности IoT-инфраструктуры?
52. В чем заключается ответственность производителей IoT-устройств согласно новым законодательным инициативам (например, закону Калифорнии или Cyber Resilience Act EC)?
53. Какая проблема может возникнуть при запрете использования стандартных паролей на IoT-устройствах?
54. Каковы прогнозы по росту количества IoT-устройств к 2025 году?
55. Как развитие технологий 5G и Edge Computing влияет на безопасность IoT?
56. Каким образом искусственный интеллект (AI) может быть использован для защиты IoT-систем?
57. Как технология блокчейн может повысить безопасность данных в IoT?
58. Что такое «сложные цепочки поставок» и какие риски для безопасности IoT они создают?
59. Какие новые вызовы в области безопасности IoT ожидаются в 2025 году согласно прогнозам?
60. Какие ключевые выводы о будущем безопасности IoT представлены в заключении лекции?

Атаки С ИСПОЛЬЗОВАНИЕМ DNS1.3

Введение в тему подмены DNS
1.1. Сущность системы доменных имен DNS и ее роль в сети Интернет.
1.2. Атаки подмены DNS.
Цели подмены DNS
Примеры использования подмены DNS злоумышленниками
Последствия подмены DNS 5
2. Механизмы подмены DNS
2.1. Способы подмены DNS: обзор методов (например, через вредоносное ПО, атаки типа Man-in-the-Middle).
Основные методы подмены DNS
Атаки типа Man-in-the-Middle (MitM)
Меры предосторожности
2.2. Инструменты для подмены DNS: программное обеспечение и техники, используемые злоумышленниками.
Основные методы подмены DNS
Инструменты управления DNS
Меры предосторожности
3. Последствия подмены DNS
3.1. Влияние на пользователей: как подмена DNS может угрожать безопасности и конфиденциальности.
Методы атаки
Конфиденциальность данных
Отсутствие аутентификации DNS
Воздействие атак
3.2. Экономические последствия: ущерб для бизнеса и репутации.
Финансовые потери
Репутационные риски
4. Примеры подмены DNS
4.1. Известные инциденты: анализ нескольких случаев подмены DNS в истории.
4.2. Уроки практики противодействия.
5. Защита от подмены DNS
5.1. Технологии защиты: использование DNSSEC и других методов.

5.2. Рекомендации для пользователей: советы по повышению безопасности.
Выбор надежного VPN-сервиса
Обеспечение защиты от утечек DNS
Использование DNSSEC
Настройка DoH и DoT
Выбор правильного DNS-сервера
Регулярные обновления и мониторинг

Контрольные вопросы

1. Какова основная функция системы доменных имен (DNS) в интернете?
2. Почему DNS часто сравнивают с «телефонной книгой» интернета?
3. Что такое «подмена DNS» (DNS Spoofing) и какова ее основная цель?
4. Назовите и кратко охарактеризуйте четыре основные цели атак с подменой DNS.
5. Как фишинг связан с подменой DNS?
6. Каким образом подмена DNS может привести к установке вредоносного ПО на устройство пользователя?
7. Как атаки типа «отказ в обслуживании» (DoS) используют подмену DNS?
8. Опишите метод «отравления кэша DNS» (DNS Cache Poisoning).
9. В чем заключается суть атаки «перехват DNS» (DNS Hijacking)?
10. Что такое «DNS туннелирование» (DNS Tunneling) и для каких целей оно используется?
11. Как работает атака «подмена DNS-сообщений»?
12. Что такое атака «человек посередине» (MitM) в контексте DNS?
13. Как злоумышленники используют фальшивые точки доступа Wi-Fi для подмены DNS?
14. Что такое ARP-отравление и какую роль оно играет в атаках на DNS?
15. Какие инструменты управления DNS (например, Cloudflare, Amazon Route 53) могут использоваться для защиты?
16. Почему протокол DNSSEC критически важен для защиты от подмены DNS?
17. Каковы основные последствия подмены DNS для конфиденциальности данных пользователя?
18. Как подмена DNS используется в фишинговых схемах для кражи личных данных?
19. Почему традиционный протокол DNS считается уязвимым из-за отсутствия аутентификации?
20. Согласно отчету «2023 Global DNS Threat Report», какой процент организаций столкнулся с DNS-атаками и каков был средний финансовый ущерб?
21. Каковы прямые финансовые потери для бизнеса в результате атак с подменой DNS?
22. Как подмена DNS может нанести репутационный ущерб компании?
23. Опишите инцидент подмены DNS, связанный с компанией Google в 2010 году.
24. Чем была знаменита атака на компанию Dyn в 2016 году и какие сервисы пострадали?
25. Как в атаке на Equifax (2017) была использована подмена DNS?
26. Какой урок можно извлечь из инцидента с Facebook в 2019 году, связанного с подменой DNS?
27. Каковы ключевые уроки по противодействию подмена DNS, вынесенные из анализа реальных инцидентов?
28. Какую роль в защите от подмены DNS играет обучение сотрудников и пользователей?
29. Почему многофакторная аутентификация является важной мерой защиты, даже если произошла подмена DNS?
30. Как системы обнаружения вторжений (IDS) и анализ логов помогают в борьбе с подменой DNS?
31. Что такое DNSSEC и какие две основные функции безопасности он обеспечивает?
32. Какие статистические данные о развертывании DNSSEC были представлены на конференции ICANN81?
33. Что такое запись DS (Delegation Signer) в контексте DNSSEC?
34. Как технология DANE (DNS-based Authentication of Named Entities) использует DNS для повышения безопасности?
35. Почему автоматизация управления ключами и записями важна для эффективного использования DNSSEC?
36. Как протоколы DNS-over-HTTPS (DoH) и DNS-over-TLS (DoT) повышают безопасность DNS?
37. В чем разница между DoH и DoT?

38. Почему использование надежного VPN-сервиса считается эффективной мерой защиты от подмены DNS?
39. Что такое «утечка DNS» и как от нее защититься при использовании VPN?
40. Какие преимущества для безопасности дает использование публичных DNS-серверов, таких как Cloudflare или Google?
41. Как пользователь может проверить и изменить настройки DNS на своем устройстве?
42. Почему регулярное обновление операционной системы и приложений важно для защиты от атак на DNS?
43. Какие инструменты мониторинга DNS-трафика можно использовать для выявления аномалий?
44. Как ботнет Mirai, известный по DDoS-атакам, связан с проблемами безопасности DNS?
45. Какая связь существует между подменой DNS и кражей личных данных?
46. Как злоумышленники могут использовать скомпрометированные DNS-серверы для масштабных атак?
47. Почему безопасность DNS особенно важна для финансовых организаций и интернет-магазинов?
48. Как подмена DNS может быть использована для цензуры или блокировки доступа к информации?
49. Каковы глобальные тенденции в развитии киберугроз, связанных с DNS, согласно прогнозам на 2025 год?
50. Какова роль организации ICANN в поддержании безопасности и стабильности глобальной системы DNS?
51. Что такое «ресолвер» DNS и почему безопасность ресолвера важна для конечного пользователя?
52. Как технология RPKI (Resource Public Key Infrastructure) дополняет DNSSEC в обеспечении безопасности интернет-маршрутизации?
53. Почему рекомендуется отключать автоматическое подключение к открытым сетям Wi-Fi для защиты от подмены DNS?
54. Как веб-браузеры помогают пользователям защититься от фишинговых сайтов, на которые может перенаправить подмена DNS?
55. Что должно быть первым действием пользователя при подозрении, что его DNS был скомпрометирован?
56. Как корпоративные политики безопасности могут помочь в предотвращении атак с подменой DNS внутри организации?
57. В чем заключаются основные проблемы или сложности, связанные с повсеместным внедрением DNSSEC?
58. Как протокол HTTPS (а не HTTP) на веб-сайтах помогает mitigate последствия успешной подмены DNS?
59. Каковы основные выводы лекции о текущем состоянии и будущем угроз, связанных с подменой DNS?
60. Назовите три самых важных, на ваш взгляд, рекомендации для рядового пользователя по защите от атак с использованием DNS.

АТАКИ ТИПА СПУФИНГ 1.3

1.1. Сущность спуфинга.
1.2. Актуальность проблемы борьбы со спуфингом.
2. Типы спуфинг атак
2.1. IP-спуфинг.
2.2. MAC-адрес спуфинг.
2.3. DNS-спуфинг.
2.4. ARP-спуфинг.
2.5. Спуфинг электронной почты.
2.6. Спуфинг социального инжиниринг.
3. Методы защиты от спуфинг атак
3.1. Проверка подлинности IP-адресов.
3.2. Использование брандмауэров.
3.3. Внедрение системы обнаружения вторжений.
3.4. Проверка подлинности MAC-адресов.
3.5. Использование DNSSEC.

3.6. SPF, DKIM, DMARC для защиты от спуфинга электронной почты.
3.7. Обучение пользователей.
4. Примеры спуфинг атак и их последствия
4.1. Краткое описание нескольких известных случаев атак.
4.2. Анализ последствий атак.

Контрольные вопросы

1. Что такое спуфинг в контексте кибербезопасности?
2. Какие основные цели преследуют злоумышленники при использовании спуфинга?
3. Почему спуфинг считается одной из самых серьезных угроз в кибербезопасности?
4. Какие типы спуфинга существуют?
5. Как спуфинг связан с фишингом?
6. Что такое IP-спуфинг и как он работает?
7. Какие последствия может иметь IP-спуфинг для сетевой инфраструктуры?
8. Как злоумышленники используют IP-спуфинг для атак типа DoS?
9. Что такое MAC-адрес спуфинг и как он осуществляется?
10. Какие последствия может иметь MAC-адрес спуфинг для локальной сети?
11. Что такое DNS-спуфинг и как он используется в атаках?
12. Какие методы используются для отравления DNS-кэша?
13. Что такое ARP-спуфинг и как он работает?
14. Какие последствия может иметь ARP-спуфинг для сетевого трафика?
15. Как злоумышленники используют спуфинг электронной почты?
16. Какие методы используются для подделки адреса отправителя в электронной почте?
17. Что такое спуфинг социального инжиниринга и как он связан с психологическим воздействием?
18. Какие примеры атак социального инжиниринга с использованием спуфинга вы можете привести?
19. Какие методы используются для проверки подлинности IP-адресов?
20. Как работает фильтрация на основе IP-адресов (Ingress и Egress фильтрация)?
21. Как брандмауэры помогают защититься от спуфинга?
22. Какие функции выполняют системы обнаружения и предотвращения вторжений (IDS/IPS) в контексте защиты от спуфинга?
23. Как протокол IPsec помогает защититься от IP-спуфинга?
24. Какие меры защиты используются для предотвращения MAC-адрес спуфинга?
25. Что такое DNSSEC и как он защищает от DNS-спуфинга?
26. Какие преимущества и недостатки имеет DNSSEC?
27. Как работают протоколы SPF, DKIM и DMARC для защиты от спуфинга электронной почты?
28. Какие шаги необходимы для настройки SPF, DKIM и DMARC?
29. Почему обучение пользователей основам информационной безопасности важно для защиты от спуфинга?
30. Какие методы обучения наиболее эффективны для повышения осведомленности о спуфинге?
31. Какие известные случаи атак, связанных со спуфингом, вы можете привести?
32. Как атака на MOVEit в 2023 году связана с методами спуфинга?
33. Какие последствия имела атака на MGM Resorts в 2023 году?
34. Как злоумышленники использовали социальную инженерию в атаке на 23andMe?
35. Какие финансовые потери могут возникнуть в результате успешной атаки спуфинга?
36. Как спуфинг может привести к утечке конфиденциальной информации?
37. Какие репутационные риски возникают у компаний после успешной атаки спуфинга?
38. Какие юридические последствия могут возникнуть в результате атак спуфинга?
39. Какие основные принципы защиты от спуфинга вы можете назвать?
40. Почему спуфинг остается актуальной угрозой в современном мире?
41. Какие технологии будущего могут помочь в борьбе со спуфингом?
42. Как искусственный интеллект может быть использован для обнаружения атак спуфинга?
43. Какие меры безопасности должны быть приняты для защиты корпоративных сетей от спуфинга?
44. Как концепция "нулевого доверия" (Zero Trust) помогает защититься от спуфинга?

45. Какие уязвимости в сетевых протоколах могут быть использованы для спуфинга?
46. Как спуфинг может быть использован для атак на беспилотные летательные аппараты?
47. Какие методы защиты от спуфинга наиболее эффективны для небольших компаний?
48. Как спуфинг может быть использован для атак на IoT-устройства?
49. Какие меры защиты от спуфинга должны быть приняты в облачных средах?
50. Как спуфинг может быть использован для атак на VPN?
51. Какие методы защиты от спуфинга наиболее эффективны для защиты персональных данных?
52. Как спуфинг может быть использован для атак на системы GPS?
53. Какие меры защиты от спуфинга должны быть приняты в банковской сфере?
54. Как спуфинг может быть использован для атак на системы электронной коммерции?
55. Какие меры защиты от спуфинга должны быть приняты в государственных учреждениях?
56. Как спуфинг может быть использован для атак на системы здравоохранения?
57. Какие меры защиты от спуфинга должны быть приняты в образовательных учреждениях?
58. Как спуфинг может быть использован для атак на системы энергетики?
59. Какие меры защиты от спуфинга должны быть приняты в транспортной сфере?
60. Как спуфинг может быть использован для атак на системы связи?

АТАКИ_И_ЭКСПЛОЙТЫ_НУЛЕВОГО_ДНЯ_1_2 (3)

. Введение в тему эксплойтов нулевого дня
1.1. Определение эксплойта нулевого дня.
1.2. Исторический контекст: краткий обзор развития эксплойтов нулевого дня.
2. Механизм работы эксплойтов нулевого дня
2.1. Уязвимости программного обеспечения.
Причины возникновения уязвимостей
Методы обнаружения уязвимостей
2.2. Процесс эксплуатации.
Методы эксплуатации уязвимостей нулевого дня
Процесс атаки
Организованная киберпреступность и уязвимости нулевого дня.
Примеры уязвимостей 2024 года
3. Примеры известных эксплойтов нулевого дня
3.1. Пример 1
Последствия эксплуатации CVE-2023-28121
3.2. Пример 2
3.3. Пример 3
4. Средства защиты от эксплойтов нулевого дня
4.1. Обновление программного обеспечения.
4.2. Использование антивирусов и систем обнаружения вторжений.
Антивирусные решения
Системы обнаружения вторжений
Принципы работы IDS/IPS
4.3. Обучение пользователей.
Актуальность обучения
Программы повышения осведомленности
Рекомендации по реализации программ
5. Будущее эксплойтов нулевого дня
5.1. Тенденции в области кибербезопасности.
5.2. Роль искусственного интеллекта в борьбе с эксплойтами.

Контрольные вопросы

1. Что такое эксплойт нулевого дня?
2. Почему эксплойты нулевого дня считаются особенно опасными?
3. Какие уязвимости были использованы в эксплойтах нулевого дня в 2023 году?
4. Как уязвимость CVE-2023-0669 в GoAnywhere MFT повлияла на организации?

5. Какие данные свидетельствуют о росте числа уязвимостей в 2023 году?
6. Какие исторические примеры использования эксплойтов нулевого дня известны?
7. Как червь Stuxnet использовал эксплойты нулевого дня для атаки на ядерные объекты?
8. Какие уязвимости использовала группа хакеров HAFNIUM в 2021 году?
9. Как изменилось количество эксплойтов нулевого дня в 2023 году по сравнению с предыдущими годами?
10. Какие методы используются для обнаружения уязвимостей в программном обеспечении?
11. Какие факторы способствуют возникновению уязвимостей в программном обеспечении?
12. Как работает метод обнаружения уязвимостей на основе сигнатур?
13. Какие инструменты используются для автоматического сканирования уязвимостей?
14. Как злоумышленники используют дизассемблирование кодов для обнаружения уязвимостей?
15. Какие методы применяются для эксплуатации уязвимостей нулевого дня?
16. Как организованная киберпреступность использует уязвимости нулевого дня?
17. Какие уязвимости нулевого дня были активно эксплуатированы в 2024 году?
18. Какие последствия может иметь уязвимость CVE-2024-35178 в Jupyter Notebooks?
19. Как уязвимость CVE-2023-28121 в WooCommerce Payments повлияла на бизнесы?
20. Какие финансовые потери могут возникнуть из-за эксплуатации уязвимостей нулевого дня?
21. Как уязвимость CVE-2023-27997 в FortiOS повлияла на безопасность систем?
22. Почему регулярные обновления программного обеспечения важны для защиты от эксплойтов нулевого дня?
23. Какие риски связаны с использованием устаревшего программного обеспечения?
24. Как автоматизация обновлений помогает повысить безопасность систем?
25. Какие антивирусные программы считаются наиболее эффективными в 2024 году?
26. Как системы обнаружения вторжений (IDS/IPS) помогают защитить от эксплойтов нулевого дня?
27. Какие популярные системы IDS/IPS используются для защиты сетей?
28. Как искусственный интеллект может помочь в борьбе с эксплойтами нулевого дня?
29. Какие методы анализа уязвимостей использует искусственный интеллект?
30. Как AI может автоматизировать процессы реагирования на киберугрозы?
31. Какие тенденции в области кибербезопасности ожидаются в 2025 году?
32. Как злоумышленники могут использовать открытые исходники для атак?
33. Какие угрозы связаны с использованием AI-технологий в кибератаках?
34. Как организации могут защититься от атак, использующих дипфейки?
35. Какие меры могут помочь предотвратить атаки на не поддерживаемое программное обеспечение?
36. Как обучение пользователей помогает снизить риски, связанные с эксплойтами нулевого дня?
37. Какие программы повышения осведомленности о кибербезопасности считаются эффективными?
38. Как компании могут оценить эффективность своих программ обучения по кибербезопасности?
39. Какие рекомендации по внедрению программ повышения осведомленности о безопасности?
40. Как искусственный интеллект может улучшить разработку безопасного программного обеспечения?

БЭКДОР 1.3

1.1. Определение бэкдора: типы и классификация.
1.2. Актуальность темы: угрозы безопасности и экономический ущерб.
2. Механизмы реализации бэкдоров
2.1. Бэкдоры на уровне операционной системы.
2.2. Бэкдоры в программном обеспечении.
2.3. Бэкдоры в аппаратном обеспечении (hardware backdoors).
2.4. Социальная инженерия как метод внедрения бэкдоров.
3. Методы обнаружения бэкдоров
3.1. Статический анализ кода.
3.2. Динамический анализ поведения системы.
3.3. Системный мониторинг и анализ журналов.
3.4. Использование специализированного ПО для обнаружения бэкдоров.
4. Методы защиты от бэкдоров
4.1. Безопасное программирование и разработка ПО.
4.2. Регулярное обновление программного обеспечения.

4.3. Использование антивирусных и анти-malware решений.
4.4. Контроль доступа и управление привилегиями.
4.5. Обучение персонала основам информационной безопасности.
5. Правовые аспекты использования и обнаружения бэкдоров
5.1. Законодательство о киберпреступлениях.
5.2. Ответственность за создание и использование бэкдоров.
6. Примеры реальных случаев использования бэкдоров
6.1. Известные случаи взлома систем с использованием бэкдоров.
6.2. Анализ последствий и уроков из реальных случаев.

Контрольные вопросы

1. Дайте определение бэкдора в контексте кибербезопасности.
2. Чем основная функция бэкдора отличается от вируса или троянской программы?
3. Назовите три основных критерия классификации бэкдоров.
4. Что такое программный бэкдор и каковы его основные разновидности?
5. Приведите примеры троянских программ, используемых в качестве бэкдоров.
6. Чем опасны корневые комплекты (Rootkits) по сравнению с другими типами бэкдоров?
7. Как бэкдоры могут быть внедрены через легитимные обновления ПО?
8. Что такое аппаратный бэкдор и почему его сложно обнаружить?
9. Каким образом сетевые бэкдоры позволяют контролировать трафик?
10. Какую статистику по использованию бэкдоров в кибератаках приводит отчет IBM Security X-Force?
11. Какова связь между бэкдорами и последующими атаками программ-вымогателей?
12. Почему бэкдоры представляют экономическую угрозу для бизнеса?
13. В чем заключается основное преимущество бэкдора, внедренного на уровне операционной системы?
14. Какими способами может быть осуществлено внедрение бэкдора на уровне ОС?
15. Приведите примеры известных бэкдоров на уровне ОС (например, SysJoker, ShadowPad).
16. Какую угрозу представляют кернел-уровневые бэкдоры?
17. Проанализируйте атаку на MOVEit Transfer с точки зрения использования уязвимостей для внедрения бэкдора.
18. Какие тенденции в использовании шпионского ПО с функциями бэкдоров отмечались в 2023 году?
19. Что такое бэкдор BrockenDoor и на какие организации он был нацелен?
20. Каковы основные причины появления аппаратных бэкдоров?
21. Чем преднамеренно внедренный аппаратный бэкдор отличается от производственного дефекта?
22. Почему проблема прозрачности цепочек поставок критична для защиты от аппаратных бэкдоров?
23. Какую роль в внедрении бэкдоров играет социальная инженерия?
24. Какую статистику по успешности атак с использованием социальной инженерии приводит Positive Technologies?
25. Опишите механизм фишинговой атаки для внедрения бэкдора.
26. Что такое вишинг и смишинг и как они используются для установки бэкдоров?
27. В чем заключается суть метода «обратной социальной инженерии»?
28. Как искусственный интеллект повышает эффективность атак социальной инженерии?
29. Что такое статический анализ кода (SAST) и как он помогает в обнаружении бэкдоров?
30. Назовите три популярных инструмента для статического анализа кода и их ключевые особенности.
31. Что такое динамический анализ поведения системы и какие методы он включает?
32. Какие признаки в активных процессах могут указывать на наличие бэкдора?
33. Как анализ системных журналов помогает в обнаружении несанкционированной активности?
34. Какие специализированные программы (например, Rootkit Hunter, Lynis) используются для поиска бэкдоров и руткитов?
35. Как сканирование сети и портов может выявить сетевую активность бэкдора?
36. Какую роль в обнаружении бэкдоров играют искусственный интеллект и аналитика больших данных?
37. Каковы challenges мониторинга безопасности в распределенных и облачных средах?
38. Какие категории специализированного ПО используются для обнаружения бэкдоров?

39. В чем ограничения антивирусных решений, таких как ClamAV, в обнаружении бэкдоров?
40. Как системы обнаружения вторжений (IDS), подобные Snort, помогают выявлять бэкдоры?
41. Как инструменты анализа целостности системы (Tripwire, AIDE) обнаруживают изменения, связанные с бэкдорами?
42. Что такое принцип «Shift-left Security» в контексте безопасной разработки ПО?
43. Какие распространенные уязвимости кода (из OWASP Top 10) могут быть использованы для внедрения бэкдоров?
44. Как выбор языка программирования (например, Rust) может повлиять на безопасность ПО?
45. Какую роль в предотвращении бэкдоров играют SAST, DAST и SCA?
46. Почему регулярное обновление программного обеспечения является критически важной мерой защиты?
47. Какие последствия могут быть у атак, эксплуатирующих уязвимости в устаревшем ПО (на примере WannaCry)?
48. Какую статистику по атакам на устаревшее ПО приводит отчет за 2023 год?
49. Каковы ограничения антивирусных решений в борьбе с современными бэкдорами?
50. Почему защита в реальном времени является важной функцией антивирусного ПО для противодействия бэкдорам?
51. Что такое контроль доступа и как его модели (DAC, MAC, RBAC) помогают защититься от бэкдоров?
52. Каковы ключевые функции систем управления привилегированным доступом (PAM)?
53. Как поведенческая аналитика в PAM-системах помогает выявлять подозрительную активность?
54. Почему обучение персонала является критическим элементом защиты от бэкдоров, внедряемых через социальную инженерию?
55. Какие российские законы (№149-ФЗ, №152-ФЗ) регулируют вопросы защиты от кибератак, связанных с бэкдорами?
56. Какие статьи Уголовного кодекса РФ могут быть применены к создателям и пользователям бэкдоров?
57. Как международное законодательство (например, Регламент ЕС о кибербезопасности) борется с угрозой бэкдоров?
58. Проанализируйте известный случай взлома с использованием бэкдора (например, SolarWinds, атака на MOVEit).
59. Какие ключевые уроки по защите от бэкдоров можно извлечь из анализа реальных инцидентов?
60. Сформулируйте основные выводы лекции о комплексном подходе к защите от бэкдоров.

ИНЪЕКЦИИ-1.3 (2)

1.1. Определение понятия “инъекция” в контексте программирования.
1.2. Актуальность проблемы SQL-инъекций и других типов.
2.2. Типы инъекций
2.1. SQL-инъекции: механизм, примеры, последствия.
2.2. XSS инъекции.
2.3. Инъекции командной строки (OS injection).
2.4. Другие типы инъекций.
3.3. Методы защиты от инъекций
3.1. Параметризованные запросы (prepared statements) и их преимущества.
3.2. Валидация и санитазация входных данных.
3.3. Использование экранирования специальных символов.
3.4. Принцип наименьших привилегий (Principle of Least Privilege).
3.5. Web Application Firewalls (WAF).
4.4. Практические примеры уязвимостей и методы их реализации
4.1. Демонстрация SQL-инъекции на примере простого веб-приложения.
4.2. Анализ реальных примеров уязвимостей из баз данных CVE.
5.5. Современные подходы к борьбе с инъекциями
5.1. Static Application Security Testing и Dynamic Application Security Testing.
5.2. Инструменты для автоматического поиска уязвимостей.
5.3. Роль разработчиков и тестировщиков в предотвращении инъекций.

Контрольные вопросы

1. Что такое инъекция в программировании, и какие её основные виды существуют?
2. Почему инъекции представляют серьёзную угрозу для безопасности приложений?
3. Почему SQL-инъекции остаются одной из самых опасных уязвимостей веб-приложений?
4. Какие последствия может вызвать успешная SQL-инъекция для компании и пользователей?
5. Как злоумышленники используют SQL-инъекции для обхода аутентификации?
6. Какие методы защиты помогают предотвратить атаки с использованием SQL-инъекций?
7. В чем различие между сохраненными, отраженными и DOM-based XSS-атаками?
8. Какие последствия могут возникнуть в результате успешной XSS-атаки?
9. Как злоумышленники используют инъекции командной строки (OS Injection) для выполнения произвольных команд?
10. Какие последствия может вызвать успешная атака с использованием OS Injection?
11. Как XML-инъекции (XXE) могут привести к утечке данных или удаленному выполнению кода?
12. Какие механизмы защиты помогают предотвратить XML-инъекции?
13. Как злоумышленники используют LDAP-инъекции для обхода аутентификации?
14. Какие методы защиты от LDAP-инъекций наиболее эффективны?
15. Почему параметризованные запросы (prepared statements) считаются одним из лучших способов защиты от SQL-инъекций?
16. В чем разница между валидацией и санитизацией входных данных?
17. Почему принцип наименьших привилегий (PoLP) играет важную роль в защите от атак?
18. Какие преимущества даёт использование Web Application Firewall (WAF) в защите от инъекционных атак?
19. Какие уязвимости, связанные с инъекциями, наиболее часто встречаются в базе данных CVE?
20. Какие примеры реальных атак с использованием SQL-инъекций были зафиксированы в последние годы?
21. Как статическое тестирование безопасности (SAST) помогает выявлять уязвимости в коде?
22. В чем отличие статического (SAST) и динамического (DAST) тестирования безопасности приложений?
23. Какие инструменты используются для автоматического поиска уязвимостей, связанных с инъекциями?
24. Какую роль разработчики играют в предотвращении инъекционных атак?
25. Почему тестирование на проникновение (пентест) является важной частью защиты от инъекций?
26. Какой комплексный подход к защите от инъекций считается наиболее эффективным?
27. Какие современные тенденции в области безопасности помогают снижать риски инъекционных атак?
28. Почему регулярное обновление программного обеспечения критично для защиты от уязвимостей?
29. Какие наиболее распространенные ошибки допускают разработчики, приводящие к уязвимостям?
30. Как искусственный интеллект может помочь в обнаружении инъекционных атак?
31. Как атаки XSS могут использоваться для кражи данных пользователей?
32. В чем разница между OS-инъекциями и SQL-инъекциями?
33. Какие методы защиты помогают предотвратить инъекции командной строки (OS Injection)?
34. Как работает механизм XML-инъекций (XXE), и какие риски он несет?
35. Почему LDAP-инъекции могут привести к несанкционированному доступу к системе?
36. Какие методы защиты наиболее эффективны против LDAP-инъекций?
37. Как принципы безопасного программирования помогают предотвращать инъекционные атаки?
38. Почему важно сочетать разные методы защиты для обеспечения безопасности приложений?

КЕЙЛОГЕР 1.3 (2)

1. Определение keylogger’а и его основные типы

1.1. Что такое keylogger? Различные определения и классификации.

1.2. Типы keylogger’ов: программные, аппаратные, программные с использованием скрытых возможностей ОС. Примеры.

2. Механизмы работы keylogger’ов

2.1. Запись нажатий клавиш: методы перехвата событий клавиатуры на разных уровнях (драйверы, API).

2.2. Запись других действий пользователя: перехват буфера обмена, скриншоты, запись аудио.
2.3. Методы скрытия keylogger’ов: маскировка файлов, автозагрузка, rootkits.
3. Распространение keylogger’ов
3.1. Вредоносные программы и трояны.
3.2. Фишинговые атаки и социальная инженерия.
3.3. Зараженные сайты и приложения.
3.4. Подключение к незащищенным Wi-Fi сетям.
4. Защита от keylogger’ов
4.1. Программные средства защиты: антивирусы, анти-keylogger’ы.
4.2. Аппаратные средства защиты: использование защищенных клавиатур.
4.3. Меры предосторожности: безопасное использование интернета, осторожность при открытии файлов, регулярное обновление программного обеспечения.
4.4. Мониторинг системы на предмет подозрительной активности.
5. Правовые аспекты использования keylogger’ов
5.1. Законодательство о киберпреступлениях.
5.2. Ответственность за использование keylogger’ов.
5.3. Этические аспекты мониторинга сотрудников.

Контрольные вопросы

1. Дайте определение кейлоггера (keylogger) и сформулируйте его основную цель.
2. Назовите два основных типа кейлоггеров по способу реализации.
3. В чем заключается ключевое различие между программными и аппаратными кейлоггерами?
4. Перечислите не менее четырех разновидностей программных кейлоггеров.
5. Что такое кейлоггеры на уровне ядра (Kernel-based) и чем они опасны?
6. Как работают веб-кейлоггеры (Web-based keyloggers)?
7. Опишите принцип действия аппаратного кейлоггера, подключаемого между клавиатурой и компьютером.
8. Каковы преимущества и недостатки перехвата нажатий клавиш на уровне драйверов?
9. Каковы преимущества и недостатки перехвата нажатий клавиш на уровне API?
10. Почему перехват на уровне драйверов считается более мощным, но и более сложным в реализации?
11. Какие методы, помимо записи нажатий клавиш, используют современные кейлоггеры для сбора информации?
12. Почему перехват буфера обмена представляет серьезную угрозу безопасности?
13. Какую дополнительную информацию могут собирать кейлоггеры с помощью функций создания скриншотов и записи аудио?
14. Какие основные методы используются для скрытия файлов кейлоггеров в системе?
15. Как злоумышленники обеспечивают автозагрузку кейлоггера для его постоянной работы?
16. Что такое руткиты (rootkits) и какую роль они играют в маскировке кейлоггеров?
17. Приведите примеры известных руткитов, используемых для сокрытия вредоносной активности.
18. Какую статистику по росту атак с использованием банковских троянов приводят источники за 2024 год?
19. Каковы основные способы распространения троянских программ, содержащих кейлоггеры?
20. Какую роль в распространении кейлоггеров играет электронная почта?
21. Что такое фишинг и как он связан с установкой кейлоггеров?
22. Какую статистику по использованию социальной инженерии в кибератаках приводят источники?
23. Какие новые методы фишинга отмечаются в 2024 году (например, использование HTTP-заголовков, смшинг)?
24. Каковы основные цели фишинговых атак согласно статистике?
25. Каким образом зараженные веб-сайты могут способствовать установке кейлоггера на устройство пользователя?
26. Что такое драйв-бай (drive-by) атака и чем она опасна?
27. Каковы риски загрузки приложений из сторонних (неофициальных) магазинов?
28. Что такое атака «человек посередине» (Man-in-the-Middle) в контексте незащищенных Wi-Fi сетей?

29. Как злоумышленник может использовать поддельную точку доступа Wi-Fi для перехвата данных?
30. Почему использование незашифрованных сетей (открытых или с протоколом WEP) опасно с точки зрения угрозы кейлоггеров?
31. Какие современные антивирусные решения показали высокую эффективность в защите от вредоносных программ, включая кейлоггеры, по данным тестов 2024 года?
32. Почему не существует отдельной категории ПО «анти-кейлоггер» и как обеспечивается защита от них?
33. Какой принцип защиты лежит в основе защищенных клавиатур от аппаратных кейлоггеров?
34. Каковы ключевые меры предосторожности для безопасного использования интернета, помогающие предотвратить заражение кейлоггером?
35. Почему регулярное обновление операционной системы и приложений критически важно для защиты?
36. Какие действия пользователя при открытии файлов могут снизить риск заражения?
37. На мониторинге каких системных событий и изменений следует сосредоточиться для обнаружения кейлоггера?
38. Как анализ сетевого трафика может помочь в выявлении кейлоггера?
39. Какие инструменты можно использовать для анализа сетевой активности на предмет подозрительных соединений?
40. Как системы обнаружения вторжений (СОВ) могут быть использованы для поиска признаков активности кейлоггеров?
41. Что такое проактивный поиск угроз (Threat Hunting) и как он применяется для обнаружения кейлоггеров?
42. Какие законодательные инициативы в области борьбы с киберпреступлениями были предложены в России в 2025 году?
43. Какие статьи Уголовного кодекса РФ могут быть применены к действиям, связанным с использованием кейлоггеров?
44. Какова общая динамика киберпреступлений в России по данным на 2024 год?
45. Каковы правовые рамки использования кейлоггеров в США согласно главе 119 Уголовного кодекса?
46. При каких условиях использование кейлоггера может считаться законным в некоторых юрисдикциях?
47. Какие этические принципы нарушаются при мониторинге сотрудников с помощью кейлоггеров без их согласия?
48. Почему прозрачность и информированное согласие являются ключевыми условиями любого законного мониторинга?
49. Какие потенциальные репутационные и правовые риски несет компания, использующая скрытый мониторинг сотрудников?
50. Каковы были основные выводы лекции относительно ключевых аспектов кейлоггеров?
51. Как эволюционировали функциональные возможности современных кейлоггеров по сравнению с их первоначальным предназначением?
52. Почему методы скрытия делают борьбу с кейлоггерами особенно сложной?
53. Какую роль в распространении кейлоггеров играют методы социальной инженерии?
54. Почему для защиты от кейлоггеров необходим именно комплексный подход?
55. Назовите три наиболее эффективных, на ваш взгляд, программных средства защиты от кейлоггеров.
56. Какой тип кейлоггера (программный или аппаратный) сложнее обнаружить и почему?
57. Какие преступления чаще всего совершаются с использованием данных, полученных кейлоггерами?
58. В чем заключается основная проблема правового регулирования использования кейлоггеров в мире?
59. Сформулируйте три основных правила личной кибергигиены, которые максимально защитят пользователя от угрозы кейлоггеров.
60. Какие новые тенденции в развитии кейлоггеров и методов защиты от них можно ожидать в ближайшем будущем?

КОМПЬЮТЕРНЫЕ_ВИРУСЫ_1_3

1.1. Сущность компьютерных вирусов.
2. Классификация компьютерных вирусов по способу заражения
2.1. Загрузочные вирусы.
2.2. Файловые вирусы.
2.3. Макровирусы.
2.4. Сетевые вирусы.
2.5. Вирусы-черви.
2.6. Троянские программы.
3. Классификация компьютерных вирусов по действиям
3.1. Неразрушающие вирусы.
3.2. Разрушающие вирусы.
3.3. Вирусы-шпионы.
3.4. Вирусы-вымогатели (ransomware).
3.5. Вирусы-ботнеты.
3.6. Полиморфные вирусы.
4. Методы защиты от компьютерных вирусов
4.1. Антивирусные программы.
4.2. Правила безопасного поведения в интернете.
4.3. Регулярное обновление программного обеспечения.

Контрольные вопросы

1. Как работают загрузочные вирусы?
2. Какие известные примеры загрузочных вирусов существовали?
3. Какие современные методы защиты от загрузочных вирусов?
4. Как заражают файлы файловые вирусы?
5. Как отличить зараженный файл от чистого?
6. Как предотвратить заражение файловыми вирусами?
7. Что такое макровирусы?
8. Как макровирусы распространяются?
9. Как отключить макросы для защиты?
10. Как сетевые вирусы распространяются?
11. Какой вирус наиболее известен среди сетевых?
12. Как защитить систему от сетевых вирусов?
13. Как черви отличаются от обычных вирусов?
14. Какие черви нанесли самый большой ущерб?
15. Как работают современные черви?
16. Чем трояны отличаются от вирусов?
17. Какие виды троянов существуют?
18. Как защититься от троянов?
19. Какие вирусы считаются неразрушающими?
20. Какой пример неразрушающего вируса?
22. Что делают разрушающие вирусы?
23. Какие разрушающие вирусы нанесли наибольший ущерб?
24. Как защититься от разрушающих вирусов?
25. Как работают вирусы-шпионы?
26. Как узнать, что на компьютере вирус-шпион?
27. Какие примеры вирусов-шпионов известны?
28. Как вирусы-вымогатели шифруют данные?
29. Какие вирусы-вымогатели стали самыми известными?
30. Что делать при заражении Ransomware?
31. Как работают ботнеты?
32. Какие примеры ботнетов существуют?
33. Как обнаружить ботнет на своем ПК?
34. Как полиморфные вирусы обходят антивирусы?

35. Как антивирусы борются с полиморфными вирусами?
36. Какой полиморфный вирус стал известным?
37. Как работают антивирусы?
38. Какие типы антивирусов существуют?
39. Как выбрать надежный антивирус?
40. Какие сайты наиболее опасны?
41. Как не заразиться вирусом через email?
42. Какие браузерные расширения помогают защите?
43. Почему важно обновлять ОС и программы?
44. Какие программы надо обновлять чаще всего?
45. Как автоматизировать обновления?
46. Какие виды резервного копирования бывают?
47. Как хранить резервные копии?
48. Как часто делать резервные копии?
49. Как работают аппаратные межсетевые экраны (firewalls)?
50. Какие протоколы используются для защиты сетей от вирусов?
51. Как IDS/IPS-системы помогают в борьбе с вирусами?
52. Почему VPN не всегда защищает от вирусов?
53. Как работает технология «песочницы» (sandboxing)?
54. Чем вредоносные DNS-серверы опасны для пользователей?
55. Как работает многофакторная аутентификация (MFA) в защите от вирусов?
56. Какие современные методы обнаружения вредоносных программ используют антивирусы?
57. Что такое поведенческий анализ в антивирусах?
58. Как антивирусы используют искусственный интеллект (ИИ)?
59. Как часто надо обновлять ПО?
60. Почему надо скрывать рекламу?

КРИПТОДЖЕКИНГ 1.3

1. Введение в криптоджекинг
1.1. Сущность криптоджекинга
1.2. Эволюция криптоджекинга
2. Технологии и методы криптоджекинга
2.1. Алгоритмы майнинга
1. SHA-256
2. Scrypt
3. Ethash
4. RandomX
5. KawPow
6. Equihash
7. Lyra2REv3
Влияние оборудования на выбор алгоритма
Программное обеспечение для майнинга
2.2. Устройства и сети, используемые для криптоджекинга.
Уязвимости в протоколах туннелирования
Устаревшее оборудование
Идентификация уязвимостей
Рекомендации по обеспечению безопасности
3. Последствия криптоджекинга
3.1. Влияние криптоджекинга на компьютеры и мобильные устройства.
Снижение производительности
Тенденции в текущем году
Рекомендации по защите
3.2. Финансовые потери пользователей и компаний.
Общие потери
Затраты на восстановление и снижение производительности
Увеличение затрат на электроэнергию

Общие убытки и компенсации
4. Защита от криптоджекинга
4.1. Методы защиты.
Топ антивирусов для защиты от криптоджекинга в текущем году:
Дополнительные рекомендации
Расширения браузеров для защиты от криптоджекинга
Встроенные механизмы защиты
4.2. Рекомендации для пользователей по защите своих устройств.
Действия при подозрении на криптоджекинг
5. Законодательство и этика
5.1. Правовые аспекты борьбы с криптоджекингом.
Основные законодательные инициативы:
Регуляции в России
Снижение рисков криптоджекинга
5.2. Моральные аспекты использования ресурсов пользователей без их ведома.
6. Будущее криптоджекинга
6.1. Тенденции развития криптоджекинга.
6.2. Новые технологии и подходы в борьбе с криптоджекингом.

Контрольные вопросы

1. Что такое криптоджекинг и как он работает?
2. Какие устройства могут быть заражены криптоджекингом?
3. Как злоумышленники заражают устройства для криптоджекинга?
4. Каковы основные признаки заражения криптоджекингом?
5. Как криптоджекинг влияет на производительность устройств?
6. Какие последствия для устройств вызывает криптоджекинг?
7. Почему криптоджекинг стал актуальной проблемой в последние годы?
8. Какие криптовалюты чаще всего майнятся с помощью криптоджекинга?
9. Как злоумышленники используют JavaScript для криптоджекинга?
10. Какие уязвимости в протоколах туннелирования используются для криптоджекинга?
11. Как устаревшее оборудование способствует распространению криптоджекинга?
12. Какие уязвимости в сетевых протоколах могут быть использованы для криптоджекинга?
13. Какие меры безопасности рекомендуются для защиты от криптоджекинга?
14. Какие антивирусные программы наиболее эффективны против криптоджекинга?
15. Какие расширения для браузеров помогают блокировать криптоджекинг?
16. Как можно защитить свои устройства от криптоджекинга?
17. Какие действия следует предпринять при подозрении на криптоджекинг?
18. Какие финансовые потери могут понести пользователи и компании из-за криптоджекинга?
19. Как криптоджекинг влияет на счета за электроэнергию?
20. Какие законодательные инициативы направлены на борьбу с криптоджекингом?
21. Как закон FIT21 в США регулирует криптовалютный рынок?
22. Какие меры принимаются в Южной Корее для защиты пользователей криптовалют?
23. Как Турция регулирует деятельность криптовалютных компаний?
24. Какие нормативные акты в России регулируют кибербезопасность и криптоджекинг?
25. Какие этические вопросы поднимает криптоджекинг?
26. Почему криптоджекинг считается морально недопустимым?
27. Какие экономические последствия имеет криптоджекинг для пользователей?
28. Как криптоджекинг влияет на углеродный след и экологию?
29. Какие тенденции развития криптоджекинга ожидаются в будущем?
30. Как искусственный интеллект может быть использован для криптоджекинга?
31. Какие новые методы атак могут появиться в криптоджекинге?
32. Как облачные инфраструктуры становятся мишенью для криптоджекинга?
33. Какие технологии используются для обнаружения и блокировки криптоджекинга?
34. Как расширения для браузеров помогают защититься от криптоджекинга?
35. Какие протоколы безопасности обновляются для борьбы с криптоджекингом?

36. Как образовательные программы помогают повысить осведомленность о криптоджекинге?
37. Как блокчейн-технологии могут быть использованы для борьбы с криптоджекингом?
38. Какие системы анализа поведения пользователей помогают выявлять криптоджекинг?
39. Как интернет-провайдеры могут помочь в борьбе с криптоджекингом?
40. Какие примеры успешных атак криптоджекинга известны?
41. Как криптоджекинг влияет на срок службы устройств?
42. Какие меры принимаются для защиты облачных сервисов от криптоджекинга?
43. Как криптоджекинг может повлиять на доверие пользователей к цифровым платформам?
44. Какие новые технологии могут быть разработаны для борьбы с криптоджекингом?
45. Как криптоджекинг может повлиять на развитие криптовалютной индустрии?
46. Какие меры безопасности могут быть внедрены в операционные системы для защиты от криптоджекинга?
47. Как криптоджекинг может повлиять на глобальное энергопотребление?
48. Какие меры могут быть приняты для снижения углеродного следа от криптоджекинга?
49. Как криптоджекинг может повлиять на развитие искусственного интеллекта?
50. Какие шаги могут предпринять пользователи для защиты своих устройств от криптоджекинга?

НЕБЕЗОПАСНАЯ-КОНФИГУРАЦИЯ-1.3 (2)

.1. Сущность понятия “небезопасная конфигурация”.
1.2. Классификация небезопасных конфигураций.
1.3. Последствия небезопасной конфигурации.
Типы небезопасных конфигураций
2.1. Небезопасные настройки операционных систем.
2.2. Небезопасные настройки сетевого оборудования.
2.3. Небезопасные настройки баз данных.
2.4. Небезопасные настройки веб-серверов и приложений.
2.5. Небезопасные настройки облачных сервисов.
Методы обнаружения небезопасных конфигураций
3.1. Автоматизированные инструменты сканирования.
3.2. Ручной аудит безопасности.
3.3. Системы мониторинга безопасности (SIEM).
4. Методы устранения небезопасных конфигураций
4.1. Применение патчей и обновлений.
4.2. Настройка правил брандмауэра.
4.3. Управление доступом (IAM).
4.4.Значение шифрования данных для защиты конфиденциальной информации.
4.5. Важность проведения пентестов для выявления уязвимостей.

Контрольные вопросы

1. Что такое небезопасная конфигурация, и почему она представляет угрозу?
2. Какие примеры небезопасных конфигураций встречаются в реальной жизни?
3. Какие основные категории небезопасных конфигураций существуют?
4. Каковы основные стандарты безопасности, связанные с конфигурацией систем?
5. Какие финансовые риски могут возникнуть из-за небезопасной конфигурации?
6. Как небезопасная конфигурация может привести к утечке данных?
7. Почему небезопасная конфигурация может нанести ущерб репутации компании?
8. Как неправильные настройки могут привести к сбоям в работе сервисов?
9. Какие уязвимости связаны с небезопасными настройками операционных систем?
10. Как отключенный брандмауэр может повлиять на безопасность системы?
11. Почему использование устаревших операционных систем является риском?
12. Какие уязвимости могут возникнуть из-за слабых паролей на сетевом оборудовании?
13. Как открытые порты могут привести к компрометации системы?
14. Какие меры можно принять для безопасной настройки сетевого оборудования?
15. Какие риски несут неправильные настройки баз данных?
16. Почему важно шифровать данные, хранящиеся в базах данных?
17. Как небезопасные настройки веб-серверов могут привести к атакам?
18. Какие распространенные уязвимости встречаются в веб-приложениях?
19. Почему отсутствие защиты от SQL-инъекций является серьезной проблемой?
20. Как XSS-атаки могут использоваться злоумышленниками?
21. Какие последствия могут возникнуть из-за отсутствия защиты от CSRF?
22. Как неправильные настройки облачных сервисов могут привести к утечке данных?
23. Какие ошибки часто допускаются при настройке IAM в облаке?
24. Почему принцип наименьших привилегий важен в облачных сервисах?
25. Какие инструменты помогают автоматизировать поиск уязвимостей конфигурации?
26. Как работает Nessus, и какие у него преимущества?
27. В чем разница между OpenVAS и QualysGuard?
28. Какие преимущества и недостатки имеет ручной аудит безопасности?
29. Как SIEM-системы помогают выявлять проблемы конфигурации?
30. Какие ключевые функции SIEM важны для обнаружения угроз?
31. Почему регулярное обновление программного обеспечения критично для безопасности?
32. Какие риски связаны с отсутствием своевременного применения патчей?
33. Как настроить брандмауэр для максимальной защиты?
34. Почему принцип минимальных привилегий важен при настройке брандмауэра?
35. Какие методы аутентификации используются в современных IAM-системах?
36. Как адаптивная MFA повышает уровень безопасности?
37. Почему аутентификация без паролей становится популярной?

38. Какие технологии позволяют реализовать концепцию Zero Trust?

39. Почему управление доступом играет ключевую роль в информационной безопасности?

40. Как шифрование помогает защитить данные от утечек?

41. Какие алгоритмы шифрования наиболее актуальны сегодня?

42. Почему квантовая криптография может стать новым стандартом безопасности?

43. Какие регуляторные требования связаны с шифрованием данных?

44. Как пентесты помогают выявлять небезопасные конфигурации?

45. Какие этапы включает процесс тестирования на проникновение?

46. Какие уязвимости чаще всего выявляются в ходе пентестов?

47. Как небезопасная конфигурация может использоваться злоумышленниками в реальных атаках?

48. Почему автоматизированные инструменты не заменяют ручной аудит?

49. Как можно минимизировать человеческий фактор при настройке систем безопасности?

50. Почему обучение персонала важно для предотвращения уязвимостей?

51. Какие тенденции в кибербезопасности помогут снизить риски конфигурационных ошибок?

52. Почему необходимо сочетание технических и организационных мер защиты?

53. Какие меры помогут предотвратить небезопасную конфигурацию в будущем?

НЕБЕЗОПАСНЫЙ_ДИЗАЙН_АРХИТЕКТУРЫ_ПРИЛОЖЕНИЯ_1_3 (2)

1.1. Сущность понятия “безопасный дизайн архитектуры”.
2. Типичные уязвимости в архитектуре приложений
2.1. Уязвимости на уровне представления (Frontend).
2.2. Уязвимости на уровне бизнес-логики.
2.3. Уязвимости на уровне данных.
2.4. Уязвимости на уровне архитектуры.
3. Принципы безопасного проектирования архитектуры
3.1. Принцип наименьших привилегий.
3.2. Разделение ответственности (separation of concerns).
3.3. Глубокая защита (defense in depth).
3.4. Использование защищенных фреймворков и библиотек.
3.5. Регулярное обновление ПО и зависимостей.
4. Методы анализа безопасности архитектуры
4.1. Статический анализ кода.
4.2. Динамический анализ кода.
4.3. Моделирование угроз.
4.4. Проверка на проникновение (Penetration Testing).
5. Практические рекомендации по созданию безопасной архитектуры
5.1. Выбор подходящей архитектуры.
5.2. Использование стандартов безопасности (OWASP, NIST).
5.3. Внедрение системы управления уязвимостями.
6. Примеры небезопасных архитектурных решений и их последствия
6.1. Примеры из реальной практики (с указанием источников).

Контрольные вопросы

1. Какие статистические данные свидетельствуют о росте киберугроз в 2024 году?
2. Какие типы вредоносного ПО наиболее активно используются злоумышленниками в 2024 году?
3. Какие финансовые последствия могут возникнуть из-за утечек данных?

4. Какие примеры утечек данных из облачных хранилищ демонстрируют проблемы небезопасного дизайна архитектуры?
5. Какие цели и задачи ставит доклад перед слушателями?
6. Что такое "безопасный дизайн архитектуры" и какие ключевые элементы он включает?
7. Какие уязвимости на уровне представления (Frontend) наиболее распространены?
8. Как работает Cross-Site Scripting (XSS) и какие методы защиты от него существуют?
9. Какие риски связаны с Cross-Site Request Forgery (CSRF) и как их можно предотвратить?
10. Какие методы защиты от SQL-инъекций через параметры URL наиболее эффективны?
11. Какие уязвимости на уровне бизнес-логики наиболее опасны?
12. Как некорректная авторизация и аутентификация могут быть использованы злоумышленниками?
13. Какие логические ошибки в бизнес-логике могут привести к уязвимостям?
14. Какие уязвимости на уровне данных наиболее критичны для безопасности приложения?
15. Как SQL-инъекции могут повлиять на целостность данных?
16. Какие проблемы с управлением доступом могут возникнуть в приложениях?
17. Какие уязвимости на уровне инфраструктуры наиболее опасны для серверов?
18. Какие последствия могут возникнуть из-за недостаточной защиты серверов?
19. Как DDoS-атаки могут повлиять на доступность приложения?
20. Что такое принцип наименьших привилегий (PoLP) и как его реализовать?
21. Какие преимущества дает реализация принципа наименьших привилегий?
22. Что такое разделение ответственности (separation of concerns) и как оно влияет на безопасность приложения?
23. Какие проблемы возникают при несоблюдении принципа разделения ответственности?
24. Что такое "глубокая защита" (defense in depth) и как она реализуется в архитектуре приложения?
25. Какие слои защиты включает в себя "глубокая защита"?
26. Какие защищенные фреймворки и библиотеки рекомендуется использовать для повышения безопасности приложения?
27. Какие рекомендации OWASP следует учитывать при выборе фреймворков и библиотек?
28. Почему регулярное обновление ПО и зависимостей критически важно для безопасности приложения?
29. Какие последствия могут возникнуть из-за использования устаревшего ПО?
30. Что такое статический анализ кода (SAST) и какие инструменты для него используются?
31. Какие ограничения имеет статический анализ кода?
32. Что такое динамический анализ кода (DAST) и как он помогает выявлять уязвимости?
33. Какие инструменты используются для динамического анализа кода?
34. Что такое моделирование угроз и как оно помогает в обеспечении безопасности приложения?
35. Какие современные вызовы в области моделирования угроз наиболее актуальны в 2024 году?
36. Что такое проверка на проникновение (Penetration Testing) и какие этапы она включает?
37. Какие тренды в пентестинге наиболее актуальны в 2024 году?
38. Какие преимущества и недостатки имеет микросервисная архитектура с точки зрения безопасности?
39. Какие преимущества и недостатки имеет монолитная архитектура с точки зрения безопасности?
40. Какие стандарты безопасности (OWASP, NIST) следует учитывать при проектировании архитектуры приложения?
41. Какие рекомендации OWASP Top 10 наиболее актуальны для разработчиков?
42. Что такое система управления уязвимостями и как её внедрить?
43. Какие принципы лежат в основе эффективного управления уязвимостями?

НЕДОЧЕТЫ-КРИПТОГРАФИИ-1.3

1.1. Этапы развития криптографии
1.2. Основные цели создания криптографических систем.
2.Уязвимости симметричной криптографии
2.1. Проблема распределения ключей
2.2. Атаки методом грубого перебора
2.3. Внутренние слабости алгоритмов
3. Уязвимости асимметричной криптографии
3.1. Проблема вычислительной сложности

3.2. Квантовые вычисления как потенциальное разрушение существующих криптосистем.
3.3. Проблемы с реализацией и управлением ключами
4.Риски реализации криптографических систем
4.1. Уязвимости криптопротоколов
4.2. Проблемы с управлением ключами и сертификатами
4.3. Опасность атак по побочным каналам
5.Перспективы развития криптографии
5.1. Горизонты постквантовой криптографии
5.2. Развитие новых алгоритмов и протоколов
5.3. Роль стандартизации и регуляторного контроля.

Контрольные вопросы

1. Какие основные этапы развития криптографии можно выделить?
2. Какую роль играют хэш-функции и цифровые подписи в современных криптосистемах?
3. В чём заключается основная цель криптографической защиты информации?
4. Почему нарушение целостности информации может привести к компрометации всей системы безопасности?
5. Какие существуют методы распределения ключей и какие их основные недостатки?
6. Почему централизованное управление ключами может представлять угрозу безопасности?
7. Как увеличение длины ключа влияет на стойкость шифра?
8. Почему квантовые компьютеры угрожают безопасности алгоритмов с короткими ключами?
9. В чём заключается угроза атак на режимы работы блочных шифров?
10. Как дифференциальный криптоанализ помогает злоумышленникам находить ключи?
11. Почему асимметричное шифрование требует больше вычислительных ресурсов, чем симметричное?
12. Как криптография на эллиптических кривых (ECC) снижает нагрузку на вычислительные мощности?
13. Почему алгоритм Шора представляет угрозу для RSA и ECC?
14. Какие криптографические алгоритмы рассматриваются как защита от квантовых атак?
15. Какие риски связаны с утечкой закрытых ключей?
16. Как вредоносное ПО может компрометировать секретные ключи?
17. Как ошибки в реализации криптографических протоколов могут ослабить их защиту?
18. Почему использование устаревших или неправильно настроенных криптобиблиотек является опасным?
19. Почему неправильное хранение и генерация ключей могут привести к компрометации системы?
20. Как можно минимизировать риски, связанные с управлением цифровыми сертификатами?
21. Какие виды атак по побочным каналам наиболее опасны для криптосистем?
22. Почему анализ энергопотребления может помочь злоумышленнику раскрыть ключ шифрования?
23. Какие криптографические методы могут быть использованы для защиты от квантовых атак?
24. Почему важно стандартизировать постквантовые криптографические алгоритмы?
25. Как развитие квантовых вычислений влияет на необходимость разработки новых алгоритмов?
26. Какие недостатки традиционных криптографических алгоритмов выявлены за последние годы?
27. Как стандартизация помогает обеспечивать безопасность криптографических систем?
28. Почему недостаточный контроль за криптографическими стандартами может привести к уязвимостям?
29. Какие основные вызовы стоят перед современной криптографией?
30. Почему квантовые технологии могут радикально изменить подход к защите информации?
31. Какие ключевые направления развития криптографии наиболее актуальны в ближайшие годы?
32. Какую роль играет обучение специалистов в обеспечении криптографической безопасности?
33. Почему криптографическая защита должна постоянно обновляться?
34. Какие технологические тенденции оказывают влияние на криптографию?
35. Как международные стандарты влияют на развитие криптографических технологий?
36. Почему внедрение новых алгоритмов требует длительного процесса тестирования и сертификации?
37. Какую роль играет сотрудничество исследовательских организаций в развитии криптографии?

38. Какие меры можно предпринять для повышения защищённости данных в условиях квантовых угроз?

ОБЕСПЕЧЕНИЕ_ПРОЦЕССА_БЕЗОПАСНОЙ_РАЗРАБОТКИ_КАК_МЕТОД_ЗАЩИТЫ_ИНФОРМАЦИИ 1.3

2. Основные принципы безопасной разработки
2.1. Shift Left.
2.2. Безопасность как услуга.
2.3. Автоматизация процессов безопасности.
3. Методы обеспечения безопасной разработки
3.1. Анализ угроз и уязвимостей.
3.2. Проектирование безопасных архитектур.
3.3. Безопасный код.
3.4. Тестирование на проникновение.
4. Инструментарий обеспечения безопасной разработки
4.1. Статический анализ кода.
4.2. Динамический анализ кода.
4.3. Инструменты для управления уязвимости.
5. Опыт применения методов безопасной разработки в различных отраслях
5.1. Примеры успешных внедрений и кейсы.
5.2. Анализ трудностей и проблем при внедрении.

Контрольные вопросы

1. Почему безопасная разработка важна для защиты информации?
2. Какова статистика уязвимостей в веб-приложениях?
3. Что такое концепция Shift Left?
4. Какие преимущества дает Shift Left?
5. Какие инструменты используются для Shift Left?
6. Как SAST интегрируется в CI/CD?
7. Какие тенденции в области Shift Left наблюдаются?
8. Что такое Security as a Service (SecaaS)?
9. Какие преимущества дает SecaaS?
10. Как Zero Trust интегрируется с SecaaS?
11. Как EDR обеспечивает безопасность конечных точек?
12. Что такое DLP и как оно защищает данные?
13. Как SecaaS помогает соответствовать регуляторным требованиям?
14. Что такое SAST (Static Application Security Testing)?
15. Какие преимущества и ограничения SAST?
16. Какие инструменты SAST существуют?
17. Что такое DAST (Dynamic Application Security Testing)?
18. Какие преимущества и ограничения DAST?
19. Как SAST и DAST дополняют друг друга?
20. Что такое DevSecOps?
21. Какие принципы DevSecOps существуют?
22. Как интегрировать безопасность в CI/CD?
23. Какие инструменты DevSecOps существуют?
24. Как управлять уязвимостями в процессе разработки?
25. Какие методы защиты контейнеров существуют?
26. Как RBAC применяется в Kubernetes?
27. Как обеспечить безопасность Infrastructure as Code?
28. Какие инструменты мониторинга контейнеров существуют?
29. Как защититься от SQL-инъекций?
30. Что такое Prepared Statements?
31. Как WAF защищает от SQL-инъекций?

32. Как защититься от XSS-атак?
33. Что такое Content Security Policy (CSP)?
34. Как escaping защищает от XSS?
35. Как защититься от CSRF-атак?
36. Что такое Anti-CSRF токены?
37. Какие практики тестирования безопасности существуют?
38. Что такое пентестирование?
39. Как часто нужно проводить пентесты?
40. Как автоматизировать тестирование безопасности?
41. Какие инструменты пентестирования существуют?
42. Что такое PT Dephaze?
43. Какие инструменты SAST рекомендуются?
44. Как работает SonarQube?
45. Как работает Veracode?
46. Как работает Checkmarx?
47. Как работает Snyk Code?
48. Какие инструменты DAST рекомендуются?
49. Как интегрировать инструменты безопасности в IDE?
50. Какие метрики оценивают безопасность кода?
51. Как обучение разработчиков повышает безопасность?
52. Какие стандарты безопасной разработки существуют?
53. Что такое OWASP и какие ресурсы они предоставляют?
54. Как использовать OWASP Top 10 для улучшения безопасности?
55. Какие правовые требования к безопасной разработке существуют?
56. Как GDPR влияет на процесс разработки?
57. Какие тенденции в области безопасной разработки ожидаются?
58. Как AI влияет на безопасную разработку?
59. Какие рекомендации по внедрению безопасной разработки можно дать?
60. Какие выводы можно сделать о роли безопасной разработки в защите информации?

ОШИБКА КОНТРОЛЯ ДОСТУПА 1.3

1.1. Актуальность проблемы ошибок контроля доступа.
2. Определение контроля доступа и его основные принципы
2.1. Основные понятия.
2.2. Модели доступа: DAC, MAC, RBAC.
2.3. Принципы безопасности.
3. Типы ошибок контроля доступа
3.1. Ошибки аутентификации.
3.2. Ошибки авторизации.
3.3. Ошибки в реализации контроля доступа.
3.4. Человеческий фактор.
4. Методы предотвращения ошибок контроля доступа
4.1. Технические методы.
4.2. Административные методы.
4.3. Организационные методы.
5. Анализ конкретных примеров ошибок контроля доступа и их последствий
5.1. Примеры реальных инцидентов.
5.2. Анализ уязвимостей и способов их эксплуатации.

1. Какова актуальность проблемы ошибок контроля доступа?
2. Какое место занимают нарушения контроля доступа в OWASP Top 10?
3. Какая статистика утечек данных за 2024 год?
4. Какие секторы наиболее уязвимы к утечкам данных?

5. Каковы финансовые последствия ошибок контроля доступа?
6. Как утечки данных влияют на репутацию компаний?
7. Что такое аутентификация?
8. Какие методы аутентификации существуют?
9. Что такое авторизация?
10. Чем авторизация отличается от аутентификации?
11. Что включает управление учетными записями?
12. Что такое ошибка контроля доступа?
13. Что такое дискреционный контроль доступа (DAC)?
14. Какие преимущества и недостатки имеет DAC?
15. Что такое обязательный контроль доступа (MAC)?
16. Какие преимущества и недостатки имеет MAC?
17. Что такое контроль доступа на основе ролей (RBAC)?
18. Какие преимущества и недостатки имеет RBAC?
19. Как выбрать подходящую модель контроля доступа?
20. В чем заключается принцип наименьших привилегий (PoLP)?
21. Как нарушение PoLP приводит к ошибкам контроля доступа?
22. Что такое разделение обязанностей (SoD)?
23. Почему важно разделять критические задачи?
24. Какие ошибки аутентификации наиболее распространены?
25. Как фишинг стал основным вектором атак?
26. Почему подбор паролей остается актуальной угрозой?
27. Какие последствия имеет кража учетных данных?
28. Какие ошибки авторизации приводят к утечкам данных?
29. Какие уязвимости авторизации были выявлены?
30. Как человеческий фактор способствует ошибкам контроля доступа?
31. Какие методы социальной инженерии используются?
32. Что такое претекстинг и «медовая ловушка»?
33. Какие технические методы предотвращения ошибок существуют?
34. Как MFA помогает защитить системы?
35. Что такое системы IDS/IPS?
36. Почему важно регулярное обновление ПО?
37. Как шифрование данных защищает от утечек?
38. Какие административные методы предотвращения существуют?
39. Как разработать эффективную политику безопасности?
40. Почему важно обучение персонала?
41. Как проводить регулярный аудит безопасности?
42. Какие организационные методы защиты существуют?
43. Как разделение обязанностей повышает безопасность?
44. Какие результаты показывают пентесты?
45. Какие примеры ошибок контроля доступа известны?
46. Как анализировать уязвимости и способы их эксплуатации?
47. Какие уязвимости были обнаружены в JIRA NASA?
48. Как неправильная конфигурация Amazon S3 привела к утечкам?
49. Какие уязвимости связаны с Citrix?
50. Что такое атака Mirai Botnet?
51. Как уязвимости кода приводят к ошибкам контроля доступа?
52. Какие инструменты используются для аудита доступа?
53. Как использовать Group Policy Management?
54. Какие метрики оценивают эффективность контроля доступа?
55. Как реагировать на инциденты, связанные с контролем доступа?
56. Какие правовые последствия влечет нарушение контроля доступа?
57. Какие стандарты регулируют контроль доступа?
58. Как внедрить Zero Trust архитектуру?
59. Какие тенденции в области контроля доступа ожидаются?
60. Какие рекомендации по улучшению контроля доступа можно дать?

ОШИБКИ_ИДЕНТИФИКАЦИИ_И_АУТЕНТИФИКАЦИИ_1_3

1.1. Проблемы ошибок идентификации и аутентификации в современном мире.
1.2. Определение основных типов ошибок, анализ причин и методов предотвращения.
2. Типы ошибок идентификации
2.1. Ошибки первого рода (ложноположительные).
2.2. Ошибки второго рода (ложноотрицательные).
2.3. Сравнение ошибок первого и второго рода.
3. Типы ошибок аутентификации
3.1. Подделка учетных данных.
3.2. Взлом системы аутентификации.
3.3. Физический доступ к устройствам аутентификации.
4. Причины ошибок идентификации и аутентификации
4.1. Слабые пароли и практики управления паролями.
4.2. Уязвимости в программном обеспечении и аппаратном обеспечении.
4.3. Человеческий фактор.
4.4. Недостаточная защита данных.
5. Методы предотвращения ошибок идентификации и аутентификации
5.1. Усиление парольной политики.
Сложные пароли.
Многофакторная аутентификация (MFA).
Рекомендации по внедрению MFA.
5.2. Регулярное обновление программного обеспечения и исправление уязвимостей.
5.3. Обучение пользователей основам кибербезопасности.
5.4. Применение современных методов аутентификации.
5.5. Защита данных.
6. Примеры реальных случаев ошибок идентификации и аутентификации и их последствия
6.1. Краткое описание нескольких известных случаев с анализом причин и последствий.

1. Что такое ошибки идентификации и аутентификации и почему они представляют серьезную угрозу?
2. Каковы прогнозируемые финансовые потери от кибератак к 2025 и 2027 году?
3. Какие известные случаи утечек данных связаны с ошибками идентификации?
4. В чем разница между идентификацией, аутентификацией и авторизацией?
5. Что такое ошибка первого рода (ложноположительный результат)?
6. Приведите примеры ложноположительных ошибок в системах безопасности.
7. Какие факторы влияют на вероятность ложноположительных ошибок?
8. Что такое ошибка второго рода (ложноотрицательный результат)?
9. Приведите примеры ложноотрицательных ошибок в системах безопасности.
10. Как качество данных влияет на вероятность ложноотрицательных ошибок?
11. Какова связь между ошибками первого и второго рода?
12. Как ROC-кривая используется для анализа ошибок идентификации?
13. Что такое подделка учетных данных и какие методы используются?
14. Какие методы подбора паролей применяют злоумышленники?
15. Что такое атака Password Spraying?
16. Что такое атака Credential Stuffing?
17. Как используется подделка биометрических данных?
18. Что такое спуфинг биометрических данных?
19. Какую угрозу представляют технологии deepfake для биометрической аутентификации?
20. Что такое подделка токенов в криптовалютах?
21. Что такое SQL-инъекции и как они связаны с ошибками аутентификации?
22. Какие последствия имели SQL-инъекции в MOVEit Transfer в 2023 году?
23. Что такое атака «человек посередине» (MITM) в контексте аутентификации?

24. Какие примеры MITM-атак произошли в последние годы?
25. Как физический доступ к устройствам может нарушить аутентификацию?
26. Какие методы клонирования карт доступа существуют?
27. Что такое SIM-своппинг и как он угрожает аутентификации?
28. Почему слабые пароли остаются актуальной проблемой?
29. Какие пароли входят в топ наиболее часто взламываемых?
30. Какие рекомендации по созданию паролей дает NIST?
31. Какие уязвимости программного обеспечения были критическими в 2023 году?
32. Что такое CVE и как классифицируются уязвимости?
33. Как человеческий фактор влияет на безопасность аутентификации?
34. Какие уязвимости связаны с недостаточной защитой данных?
35. Что такое многофакторная аутентификация (MFA)?
36. Какие типы факторов используются в MFA?
37. Как внедрить MFA в организации?
38. Почему важно регулярное обновление программного обеспечения?
39. Какие компании предлагают решения для обучения кибербезопасности?
40. Что такое беспарольная аутентификация (Passkeys)?
41. Как биометрическая аутентификация повышает безопасность?
42. Какие риски связаны с биометрической аутентификацией?
43. Что такое шифрование данных и какие алгоритмы используются?
44. Что такое HSM (Hardware Security Module)?
45. Что такое KMS (Key Management Service)?
46. Как BYOK (Bring Your Own Key) повышает безопасность?
47. Какие уроки можно извлечь из утечки данных Yahoo?
48. Какие уроки можно извлечь из утечки данных Equifax?
49. Как социальная инженерия используется для обхода аутентификации?
50. Что такое Zero Trust архитектура?
51. Какие тенденции в области аутентификации ожидаются в будущем?
52. Как квантовые вычисления могут повлиять на криптографию?
53. Какие законодательные требования регулируют защиту данных?
54. Что такое GDPR и как он влияет на аутентификацию?
55. Какова роль аудита безопасности в предотвращении ошибок?
56. Как проводить оценку рисков в системах аутентификации?
57. Какие метрики используются для оценки эффективности систем аутентификации?
58. Как обучение сотрудников помогает предотвратить ошибки аутентификации?
59. Какие инструменты мониторинга помогают обнаружить атаки на аутентификацию?
60. Какие перспективы развития систем аутентификации вы видите?

ПОДДЕЛКА_ЗАПРОСОВ_НА_СТОРОНЕ_СЕРВЕРА_1_3

1.1.Сущность подделки запросов на стороне сервера.
2. Типы подделок запросов на стороне сервера
2.1. Методы и примеры подделок HTTP-запросов.
2.2. Подделка данных в теле запроса.
2.3. Подделка IP-адреса.
3. Методы защиты от подделки запросов
3.1. Верификация данных на стороне сервера.
3.2. Использование HTTPS.
3.3. Механизмы аутентификации и авторизации.
3.4. Проверка заголовков запроса.
3.5. Функционал и возможности WAF (Web Application Firewall).
3.6. CSRF (Cross-Site Request Forgery) механизмы предотвращения.
4. Практические примеры атак и защиты
4.1. Демонстрация уязвимости в простом веб-приложении.
4.2. Демонстрация способов защиты от показанной уязвимости.
5. Современные тренды в защите от подделки запросов

5.1. Бессерверные функции и безопасность.
5.2. Использование микросервисной архитектуры для повышения безопасности.
5.3. Роль искусственного интеллекта в обнаружении атак.

1. Какова актуальность проблемы подделки запросов в 2024 году?
2. Какая статистика кибератак за 2024 год?
3. Какие CVE связаны с подделкой запросов?
4. Какие инструменты используют злоумышленники для атак?
5. Какие последствия имеют zero-day уязвимости?
6. Что такое HTTP request spoofing?
7. Как злоумышленники манипулируют GET-запросами?
8. Как злоумышленники манипулируют POST-запросами?
9. Какие HTTP-заголовки подвергаются подделке?
10. Как подделка заголовка Authorization угрожает безопасности?
11. Что такое SQL-инъекции?
12. Как Cross-Site Scripting (XSS) связан с подделкой запросов?
13. Как злоумышленники подделывают HTTP-заголовки?
14. Как подделка HTTP-методов угрожает безопасности?
15. Что такое URI manipulation?
16. Что такое IP-спуфинг?
17. Как VPN используется для подделки IP-адресов?
18. Что такое Packet Injection?
19. Как злоумышленники используют IP-спуфинг в DDoS-атаках?
20. Как обнаружить IP-спуфинг?
21. Какие методы валидации данных защищают от подделки запросов?
22. Какие хеш-функции используются для проверки целостности?
23. Как JWT защищает от подделки запросов?
24. Как анализ IP-адресов и User-Agent помогает обнаружить атаки?
25. Как HTTPS защищает от подделки запросов?
26. Какие рекомендации по внедрению HTTPS существуют?
27. Как SSL/TLS сертификаты повышают безопасность?
28. Что такое MFA и как оно защищает от атак?
29. Какие методы биометрической аутентификации существуют?
30. Как токены (JWT) используются для аутентификации?
31. Какие HTTP-заголовки безопасности существуют?
32. Как X-Frame-Options защищает от clickjacking?
33. Как Content-Security-Policy защищает от XSS?
34. Как Access-Control-Allow-Origin настраивает CORS?
35. Что такое WAF (Web Application Firewall)?
36. Какие преимущества WAF для защиты веб-приложений?
37. Как WAF защищает от SQL-инъекций и XSS?
38. Что такое CSRF (Cross-Site Request Forgery)?
39. Как CSRF-токены защищают от атак?
40. Как атрибут SameSite Cookies предотвращает CSRF?
41. Почему GET-запросы не должны изменять состояние системы?
42. Как проверка заголовков Origin и Referer помогает защите?
43. Какие примеры уязвимостей CSRF существуют?
44. Как Flask защищает от CSRF?
45. Какие методы защиты от CSRF рекомендуются?
46. Какие DevSecOps практики защищают от подделки запросов?
47. Как контейнеризация влияет на безопасность?
48. Какие инструменты сканирования уязвимостей существуют?
49. Как мониторинг runtime помогает обнаружить атаки?
50. Какие практики безопасного кодирования существуют?

51. Как защитить API от подделки запросов?
52. Какие методы аутентификации API рекомендуются?
53. Как логирование помогает обнаружить атаки?
54. Как машинное обучение используется для обнаружения атак?
55. Какие алгоритмы ML применяются для классификации атак?
56. Как обнаружить аномальный трафик с помощью ML?
57. Какие выводы можно сделать о защите от подделки запросов?
58. Какие тенденции в области защиты ожидаются?
59. Какие рекомендации по повышению безопасности можно дать?
60. Какие стандарты безопасности применяются к веб-приложениям?

ПОДСЛУШИВАЮЩИЕ АТАКИ 1.3

1. Что такое подслушивающие атаки?
2. Какие основные виды подслушивающих атак существуют?
3. Как происходит перехват данных в незашифрованных сетях?
4. Какие устройства могут быть использованы для подслушивания?
5. Как вредоносное ПО участвует в подслушивающих атаках?
6. Какие ранние методы подслушивания использовались?
7. Как развивались подслушивающие атаки с появлением электронных устройств?
8. Какие современные технологии используются в подслушивающих атаках?
9. Каковы последствия подслушивающих атак для организаций?
10. Как эволюционировали методы перехвата электромагнитных сигналов?
11. Что такое атака по словарю в контексте Wi-Fi?
12. Как работает атака на PIN-код WPS?
13. Что такое захват рукопожатия в WPA/WPA2?
14. Почему протокол WEP считается уязвимым?
15. Какие риски связаны с протоколами WPA и WPA2?
16. Как стандарт WPA3 улучшает безопасность Wi-Fi?
17. Что такое KRACK-атака?
18. Как работают атаки через фреймы управления в WPA2?
19. Что такое WiPhishing?
20. Какие методы защиты от атак на беспроводные сети существуют?
21. Что такое DDoS-атака и как она работает?
22. Как фишинг используется для подслушивания данных?
23. Какие виды вредоносного ПО применяются в подслушивающих атаках?
24. Что такое сниффинг?

25. Какие атаки на уровне приложений могут привести к утечке данных?
26. Как фильтрация трафика помогает защититься от атак?
27. Какие преимущества дает использование CDN?
28. Как облачные сервисы помогают предотвратить атаки?
29. Почему обучение пользователей важно для защиты от фишинга?
30. Какие методы защиты от атак на проводные сети существуют?
31. Что такое Tailgating в социальной инженерии?
32. Как злоумышленники устанавливают доверие с жертвой?
33. Что такое метод Quid pro quo?
34. Какую роль играет человеческий фактор в утечках данных?
35. Какие статистические данные подтверждают влияние человеческого фактора?
36. Как фишинг связан с подслушивающими атаками?
37. Какие методы манипуляции используются в телефонных атаках?
38. Как социальные сети могут быть использованы для подслушивания?
39. Какие меры защиты помогают снизить риски социальной инженерии?
40. Почему обучение сотрудников критически важно?
41. Какие физические устройства используются для подслушивания?
42. Как мобильные устройства становятся мишенями?
43. Какие технологии позволяют удаленно перехватывать данные?
44. Как электромагнитное излучение используется в подслушивающих атаках?
45. Какое влияние подслушивающие атаки оказывают на бизнес?
46. Что такое кейлоггеры и как они работают?
47. Какие функции выполняет шпионское ПО?
48. Как вредоносное ПО попадает на устройство жертвы?
49. Какие методы защиты помогают обнаружить шпионское ПО?
50. Какой процент вредоносного ПО составляет шпионское ПО?
51. Какие финансовые потери могут понести организации?
52. Как утечки данных влияют на репутацию компаний?
53. Какие примеры инцидентов, связанных с внутренними угрозами, известны?
54. Как подслушивающие атаки угрожают личной безопасности?
55. Какие уязвимости в IoT способствуют подслушиванию?
56. Какие меры помогают минимизировать риски?
57. Как двухфакторная аутентификация повышает безопасность?
58. Какие системы используются для обнаружения атак?
59. Какие юридические последствия могут возникнуть?
60. Какие этические вопросы связаны с подслушивающими атаками?

РУТКИТ 1.3

1.1. Сущность руткита
1.2.Хронология развития руткитов.
2. Типы руткитов
2.1. Классификация по способу заражения.
2.2. Классификация по цели атаки
2.3. Классификация по месту работы
2.4. Примеры известных руткитов
3. Методы обнаружения руткитов
3.1. Сигнатурный анализ.
3.2. Эвристический анализ.
3.3. Анализ поведения системы.
3.4. Использование специализированного ПО.
3.5. Ручной анализ.
4. Методы защиты от руткитов
4.1. Профилактика заражения
4.2. Регулярное сканирование системы.
4.3. Использование sandbox-технологий.

4.4. Практические рекомендации по повышению безопасности.
5. Правовые аспекты
5.1. Ответственность за создание и распространение руткитов.
5.2. Законодательство в отношении киберпреступлений.

1. Что такое руткит?
2. Какова история развития руткитов?
3. Какие известные примеры руткитов существуют?
4. Какой масштаб угрозы руткитов?
5. Какие техники MITRE ATT&CK используют руткиты?
6. Как руткиты проникают в систему?
7. Какие методы распространения руткитов существуют?
8. Как USB-устройства используются для распространения руткитов?
9. Как социальная инженерия помогает распространять руткиты?
10. Как уязвимости ПО используются для внедрения руткитов?
11. Какие типы руткитов существуют?
12. Какие функции выполняют руткиты уровня пользователя?
13. Какие функции выполняют руткиты уровня ядра?
14. Как руткиты обеспечивают скрытность?
15. Какие методы маскировки используют руткиты?
16. Какие примеры известных руткитов можно привести?
17. Что такое Stuxnet и как он работал?
18. Что такое TDSS?
19. Что такое Flame?
20. Почему сложно обнаружить руткиты?
21. Какие методы обнаружения руткитов существуют?
22. Как работает сигнатурный анализ?
23. Как работает поведенческий анализ?
24. Какие инструменты обнаружения руткитов существуют?
25. Как работает GMER?
26. Как работает RkUnhooker?
27. Какие методы анализа системных вызовов используются?
28. Какие методы анализа сетевого трафика применяются?
29. Какие антивирусные программы эффективны против руткитов?
30. Как работает Bitdefender?
31. Как работает Norton?
32. Как работает Kaspersky?
33. Какие методы ручного обнаружения руткитов существуют?
34. Как использовать отладчики для обнаружения руткитов?
35. Какие методы защиты от руткитов существуют?
36. Как антивирусы защищают от руткитов?
37. Как обновление ПО защищает от руткитов?
38. Как сканирование системы помогает обнаружить руткиты?
39. Какая оптимальная частота сканирования системы?
40. Какие результаты показывают sandbox-исследования?
41. Какие уязвимости были обнаружены в 2024 году?
42. Что такое CVE-2024-44243 в macOS?
43. Как EDR-системы помогают обнаружить руткиты?
44. Как AI используется для обнаружения руткитов?
45. Какие перспективы развития защиты от руткитов существуют?
46. Какие правовые аспекты использования руткитов существуют?
47. Какая ответственность предусмотрена по статье 272 УК РФ?
48. Какая ответственность предусмотрена по статье 273 УК РФ?
49. Какая ответственность предусмотрена по статье 274 УК РФ?

50. Какие этические вопросы связаны с руткитами?
51. Как руткиты используются в кибершпионаже?
52. Какие отрасли наиболее уязвимы к руткитам?
53. Как руткиты влияют на критическую инфраструктуру?
54. Какие рекомендации по защите от руткитов можно дать?
55. Как создать план реагирования на обнаружение руткита?
56. Какие инструменты мониторинга помогают обнаружить руткиты?
57. Как обучение сотрудников помогает предотвратить заражение руткитами?
58. Какие метрики оценивают эффективность защиты от руткитов?
59. Какие тенденции развития руткитов ожидаются?
60. Какие выводы можно сделать о защите от руткитов?

СОЦИАЛЬНАЯ_ИНЖЕНЕРИЯ_1_3

1.1. Актуальность темы социальной инженерии в современном мире.
1.2. Сущность социальной инженерии.
2. Методы социальной инженерии
2.1. Инженерия доверия
2.2. Разновидности манипуляций
2.3. Претекстинг
2.4. Квизинг
2.5. Бейтинг
2.6. Подрыв доверия
3. Примеры реальных атак социальной инженерии
3.1. Краткое описание известных случаев успешных атак.
3.2. Анализ использованных злоумышленниками уязвимостей
4. Защита от социальной инженерии
4.1. Обучение сотрудников методам распознавания и предотвращения атак.
4.2. Технические средства защиты
4.3. Политики безопасности и процедуры реагирования на инциденты.

1. Что такое социальная инженерия и почему она представляет угрозу?
2. Какие факторы способствуют росту атак социальной инженерии?
3. Как удаленная работа влияет на уязвимость к социальной инженерии?
4. Какие методы социальной инженерии наиболее распространены?
5. Каковы финансовые последствия успешных атак социальной инженерии?
6. Чем социальная инженерия отличается от технических атак?
7. Какие характеристики отличают социальную инженерию от других типов атак?
8. Что такое инженерия доверия?
9. Как злоумышленники используют имитацию авторитетных лиц?
10. Какие эмоциональные уязвимости эксплуатируют атакующие?
11. Как злоумышленники используют информацию из социальных сетей?
12. Что такое фишинг и какие его разновидности существуют?
13. Чем фишинг отличается от фарминга?
14. Что такое смишинг (Smishing)?
15. Что такое вишинг (Vishing)?
16. Что такое претекстинг?
17. Каковы последствия атак с использованием претекстинга?
18. Что такое квизинг и как он используется?
19. Какие примеры квизинговых атак можно привести?
20. Как защититься от квизинга?
21. Что такое бейтинг?
22. Какие формы бейтинга существуют?
23. Как защититься от бейтинга?

24. Что такое tailgating?
25. Каковы последствия атак tailgating?
26. Что такое shoulder surfing?
27. Какие меры предотвращают tailgating и shoulder surfing?
28. Какие примеры успешных атак социальной инженерии известны?
29. Какие уязвимости использовались в атаках на крупные компании?
30. Как обучение сотрудников помогает предотвратить атаки?
31. Какие ключевые аспекты эффективного обучения можно выделить?
32. Какие компании предлагают программы обучения по защите?
33. Что такое многофакторная аутентификация в контексте защиты от социальной инженерии?
34. Какие тенденции наблюдаются на рынке MFA?
35. Какие примеры успешного применения MFA можно привести?
36. Какие антифишинг-системы используются для защиты?
37. Как политики безопасности помогают минимизировать ущерб?
38. Какие этапы включает процедура реагирования на инциденты?
39. Какую роль играет человеческий фактор в информационной безопасности?
40. Какие меры необходимы для эффективной защиты от социальной инженерии?
41. Как создать культуру безопасности в организации?
42. Какие психологические принципы лежат в основе социальной инженерии?
43. Как злоумышленники создают чувство срочности?
44. Что такое кликбейт в контексте социальной инженерии?
45. Как распознать фишинговое письмо?
46. Какие признаки указывают на попытку социальной инженерии?
47. Как проверить легитимность запроса на конфиденциальную информацию?
48. Какие технические средства защиты от социальной инженерии существуют?
49. Как использовать симуляции атак для обучения сотрудников?
50. Какие метрики используются для оценки эффективности защиты?
51. Как изменились методы социальной инженерии с появлением ИИ?
52. Какие отрасли наиболее уязвимы к социальной инженерии?
53. Как защитить удаленных сотрудников от социальной инженерии?
54. Какие правовые последствия влечет социальная инженерия?
55. Как социальная инженерия связана с другими типами кибератак?
56. Какие инструменты используют злоумышленники для сбора информации?
57. Как защитить личную информацию в социальных сетях?
58. Какие процедуры верификации помогают противостоять претекстингу?
59. Как реагировать при обнаружении атаки социальной инженерии?
60. Какие перспективы развития методов защиты от социальной инженерии?

СРЕДСТВА_МАШИННОГО_ОБУЧЕНИЯ_КАК_ОБЪЕКТ_ЗАЩИТЫ_ИНФОРМАЦИИ_1_3

1.1. Актуальность темы защиты информации в эпоху машинного обучения.
1.2. Краткая характеристика машинного обучения и его применений.
2.2. Средства машинного обучения как уязвимые объекты
2.1. Уязвимости моделей машинного обучения.
2.2. Уязвимости данных, используемых для обучения моделей.
2.3. Уязвимости инфраструктуры, используемой для обучения и применения моделей.
3.3. Методы защиты информации, применяемые к средствам машинного обучения
3.1. Защита данных.
3.2. Защита моделей.
3.3. Защита инфраструктуры.
4.4. Практические примеры угроз и мер защиты
4.1. Пример 1.
4.2. Пример 2.
4.3. Пример 3.
5.5. Перспективы развития методов защиты информации для машинного обучения
5.1. Новые методы защиты от adversarial attacks.

5.2. Развитие технологий безопасного обмена данными для обучения моделей.
5.3. Роль законодательства в обеспечении безопасности машинного обучения.

1. Почему средства машинного обучения являются объектом защиты?
2. Какие уязвимости систем машинного обучения существуют?
3. Что такое Data Poisoning?
4. Какие последствия может иметь Data Poisoning?
5. Что такое Model Stealing?
6. Как защитить модели машинного обучения от кражи?
7. Что такое Adversarial Attacks?
8. Как состязательные атаки влияют на работу ML-систем?
9. Какие примеры состязательных атак известны?
10. Какие финансовые риски связаны с атаками на ML?
11. Какая статистика утечек данных связана с ML?
12. Как обеспечить конфиденциальность данных в ML-системах?
13. Какие методы шифрования применяются для защиты ML?
14. Что такое QKD (Quantum Key Distribution)?
15. Что такое Zero Trust Architecture в контексте ML?
16. Как SASE помогает защитить ML-системы?
17. Как EDR защищает ML-инфраструктуру?
18. Как обеспечить целостность данных в ML-системах?
19. Что такое федеративное обучение?
20. Какие преимущества федеративного обучения для безопасности?
21. Что такое Stalactite и как она обеспечивает безопасность?
22. Какие методы защиты конфиденциальности данных существуют?
23. Как дифференциальная приватность защищает данные?
24. Что такое гомоморфное шифрование?
25. Как обнаруживать вторжения в ML-системы?
26. Как IDS используется для защиты ML?
27. Как NTA помогает защитить ML-системы?
28. Что такое EDR в контексте защиты ML?
29. Какие алгоритмы ML используются для обнаружения вторжений?
30. Как SVM и kNN применяются для обнаружения атак?
31. Какие угрозы возникают при использовании открытых моделей?
32. Какие риски связаны с моделями на Hugging Face?
33. Как формат SafeTensor повышает безопасность?
34. Какие уязвимости связаны с файлами .pickle?
35. Какие сценарии атак на ML-системы существуют?
36. Как злоумышленники обходят CAPTCHA с помощью ML?
37. Какие методы защиты от adversarial attacks существуют?
38. Как регуляризация помогает защитить модели?
39. Что такое adversarial training?
40. Как аугментация данных повышает устойчивость моделей?
41. Как обнаружить отравление данных (Data Poisoning)?
42. Какие методы валидации данных применяются?
43. Как мониторинг качества данных помогает защите?
44. Какие инструменты для защиты ML-систем существуют?
45. Как Apache Kafka используется для безопасной обработки данных?
46. Как Apache Spark обеспечивает безопасность ML-пайплайнов?
47. Какие правовые аспекты связаны с защитой ML?
48. Какие стандарты безопасности применяются к ML-системам?
49. Какие этические вопросы связаны с безопасностью ML?
50. Как обеспечить прозрачность и объяснимость ML-моделей?
51. Какие угрозы создает использование AI злоумышленниками?

52. Как AI используется для создания атак?
53. Какие перспективы развития защиты ML-систем существуют?
54. Как квантовые вычисления повлияют на безопасность ML?
55. Какие рекомендации по защите ML-систем можно дать?
56. Как обучение персонала помогает защитить ML-системы?
57. Какие метрики оценивают безопасность ML-систем?
58. Как аудит безопасности применяется к ML-системам?
59. Какие тенденции в области безопасности ML ожидаются?
60. Какие выводы можно сделать о защите ML как объекта информационной безопасности?

ТРОЯНСКИЙ КОНЬ(1.3)

1. Введение в тему компьютерных вирусов
1.1. Определение компьютерного вируса: что такое вирус и как он работает.
1.2. Классификация вирусов: обзор различных типов вирусов, включая Троянских коней.
1. Виды программ-вымогателей
2. Мошеннические программы, маскирующиеся под легитимное ПО
3. Финансовые угрозы (Banking Trojans)
4. Троянские кони
5. Новые и продвинутые угрозы
2. Троянский конь: история и происхождение
2.1. Происхождение названия: мифологический контекст и его связь с компьютерной безопасностью.

Легенда о Троянском коне
Символизм термина
Мифологические архетипы и их связь с киберугрозами
2.2. Исторические примеры: известные случаи заражения и их последствия.
3. Механизмы работы Троянских коней
3.1. Способы распространения: как Троянцы проникают в системы.
Рекомендации по защите от троянов:
1. Кража данных
2. Удаленный доступ
3. Распространение других угроз
4. Атаки на системы
5. Социальная инженерия
4. Последствия заражения Троянским конем
4.1. Ущерб для пользователей: финансовые и информационные потери.
4.2. Ущерб для организаций: влияние на бизнес-процессы и репутацию.
1. Сбор и передача конфиденциальной информации
2. Установка дополнительных вредоносных программ
3. Удаленное управление компьютером
4. Мониторинг деятельности сотрудников
5. Нарушение продуктивности
5. Методы защиты от Троянских коней
5.1. Антивирусные программы: как они работают и какие функции имеют.
Основные аспекты работы антивирусных программ
Актуальные угрозы
Облачные решения и безопасность
Прогнозы
5.2. Профилактические меры: советы по безопасному поведению в сети Интернет.
6. Будущее Троянских коней и компьютерной безопасности
6.1. Эволюция угроз: как меняются методы атак и защиты.
Изменения в методах атак
Изменения в методах защиты
6.2. Роль пользователей в обеспечении безопасности: важность осведомленности и обучения.

1. Что такое троянский конь в контексте кибербезопасности?
2. Какова история происхождения термина «троянский конь»?
3. Какие типы троянов существуют?
4. Что такое ransomware-трояны?
5. Какие примеры ransomware-троянов известны?
6. Что такое Banking Trojans?
7. Какие примеры банковских троянов известны?
8. Какие основные функции выполняют трояны?
9. Как трояны распространяются?
10. Какие методы социальной инженерии используют трояны?
11. Какова история развития троянов?
12. Как работал ILOVEYOU?
13. Как работал Zeus?
14. Как работал CryptoLocker?
15. Как работал Emotet?
16. Как работал BlackEnergy?
17. Какая статистика троянских атак за 2023 год?
18. Какие трояны наиболее распространены сейчас?
19. Какие методы проникновения троянов существуют?
20. Как фишинг используется для распространения троянов?
21. Как вредоносные вложения распространяют трояны?
22. Как вредоносные ссылки распространяют трояны?
23. Как Wi-Fi-сети используются для распространения троянов?
24. Как уязвимости ПО используются для внедрения троянов?
25. Что такое RAT (Remote Access Trojan)?
26. Какие функции имеют RAT?
27. Какие примеры RAT существуют?
28. Как трояны используются для DDoS-атак?
29. Как трояны крадут данные?
30. Какой экономический ущерб наносят трояны?
31. Какая статистика финансовых потерь от кибератак?
32. Как трояны влияют на репутацию компаний?
33. Какие примеры компаний, пострадавших от троянов, известны?
34. Какие методы защиты от троянов существуют?
35. Как антивирусы защищают от троянов?
36. Как обновление ПО защищает от троянов?
37. Как обучение пользователей помогает предотвратить заражение?
38. Какие признаки заражения трояном существуют?
39. Какие методы удаления троянов существуют?
40. Как цепочка поставок используется для распространения троянов?
41. Как npm и PyPi используются для распространения троянов?
42. Какие рекомендации по безопасному поведению в сети существуют?
43. Какие перспективы развития троянов существуют?
44. Как AI влияет на развитие троянов?
45. Что такое Ransomware-as-a-Service?
46. Как IoT-устройства подвержены троянам?
47. Какие правовые аспекты связаны с троянами?
48. Какие меры принимают организации для защиты от троянов?
49. Как пентестирование помогает обнаружить уязвимости к троянам?
50. Какие инструменты мониторинга помогают обнаружить трояны?
51. Как песочницы (sandbox) используются для анализа троянов?
52. Какие метрики оценивают эффективность защиты от троянов?
53. Как реагировать на обнаружение трояна?
54. Какие планы восстановления после атаки трояна рекомендуются?

55. Как резервное копирование помогает защититься от ransomware?
56. Какие стандарты безопасности помогают защититься от троянов?
57. Как Zero Trust архитектура защищает от троянов?
58. Какие тенденции развития троянов ожидаются?
59. Какие новые методы защиты от троянов появляются?
60. Какие выводы можно сделать о защите от троянов?

УЯЗВИМОСТИ_ПРОТОКОЛОВ_ТУННЕЛИРОВАНИЯ_1_3

1.1. Сущность туннелирования и его назначение.
1.2. Типы протоколов туннелирования.
1.3. Актуальность темы уязвимостей протоколов туннелирования.
2. Уязвимости протоколов VPN
2.1. Уязвимости в реализации криптографических алгоритмов.
2.2. Уязвимости, связанные с управлением ключами.
2.3. Уязвимости на уровне протокола.
2.4. Уязвимости в клиентском ПО.
3. Уязвимости протокола SSH
3.1. Уязвимости, связанные с аутентификацией.
3.2. Уязвимости, связанные с использованием слабых паролей.
3.3. Уязвимости в реализации криптографических алгоритмов.
3.4. Уязвимости, связанные с использованием небезопасных настроек конфигурации.
4. Уязвимости протокола IPsec
4.1. Уязвимости в реализации криптографических алгоритмов.
4.2. Уязвимости, связанные с обменом ключами.
4.3. Уязвимости в реализации механизмов целостности.
5. Методы обнаружения и предотвращения уязвимостей
5.1. Проверка на уязвимости с использованием специализированных инструментов.
5.2. Регулярное обновление программного обеспечения.
5.3. Использование сильных паролей и многофакторной аутентификации.
5.4. Правильная настройка конфигурации протоколов туннелирования.
5.5. Мониторинг сетевого трафика.

1. Что такое туннелирование и каково его назначение?
2. Какие механизмы обеспечивают безопасность туннелирования?
3. В каких сценариях применяется туннелирование?
4. Какие типы протоколов туннелирования существуют?
5. Чем SSL VPN отличается от IPsec VPN?
6. Какие преимущества и недостатки имеет SSH?
7. Каковы особенности протокола IPsec?
8. Почему изучение уязвимостей протоколов туннелирования актуально?
9. Какой масштаб проблемы выявило исследование Top10VPN?
10. Какие CVE связаны с уязвимостями туннелирования?
11. Какие угрозы создают уязвимости протоколов туннелирования?
12. Какие примеры реальных атак на VPN известны?
13. Какие уязвимости криптографических алгоритмов существуют в VPN?
14. Что такое side-channel атаки?
15. Какие ошибки возникают при использовании криптографических примитивов?
16. Какие уязвимости связаны с управлением ключами в VPN?
17. Какие протоколы не обеспечивают аутентификацию корреспондентов?
18. Какие уязвимости на уровне протокола существуют?
19. Как атаки грубой силы угрожают VPN?
20. Какая критическая уязвимость обнаружена в OpenSSL?
21. Какие уязвимости клиентского ПО VPN существуют?

22. Как уязвимости ОС влияют на безопасность VPN-клиента?
23. Какие проблемы связаны с бесплатными VPN-клиентами?
24. Какие уязвимости протокола SSH связаны с аутентификацией?
25. Что такое CVE-2024-6387 (regreSSHion)?
26. Что такое Terrapin Attack?
27. Какие уязвимости SSH связаны со слабыми паролями?
28. Какие рекомендации NIST по паролям существуют?
29. Какие уязвимости криптографических алгоритмов SSH существуют?
30. Какие уязвимости связаны с небезопасными настройками SSH?
31. Какие рекомендации по настройке SSH-сервера существуют?
32. Какие уязвимости криптографических алгоритмов IPsec существуют?
33. Какие уязвимости связаны с обменом ключами в IPsec?
34. Что такое Replay Attacks в IKE?
35. Какие уязвимости механизмов целостности IPsec существуют?
36. Какие инструменты проверки на уязвимости существуют?
37. Как использовать Nmap для проверки VPN и SSH?
38. Как Metasploit Framework помогает в тестировании?
39. Как Wireshark используется для анализа уязвимостей?
40. Как Hydra используется для тестирования паролей?
41. Почему важно регулярное обновление ПО?
42. Какие уязвимости были критическими в 2024 году?
43. Какие рекомендации по созданию сильных паролей существуют?
44. Как MFA повышает безопасность туннелирования?
45. Какие рекомендации по настройке VPN существуют?
46. Как правильно настроить OpenVPN?
47. Что такое NAT-T и когда его использовать?
48. Как защитить от утечки DNS и IP-адресов?
49. Какие рекомендации по мониторингу сетевого трафика существуют?
50. Как обнаружить аномалии в сетевом трафике?
51. Какие тенденции в кибербезопасности влияют на протоколы туннелирования?
52. Что такое Terrapin и какой масштаб угрозы?
53. Какие протоколы рекомендуется использовать вместо устаревших?
54. Какие выводы можно сделать об уязвимостях протоколов туннелирования?
55. Какие меры защиты наиболее эффективны?
56. Какие тенденции влияют на развитие протоколов туннелирования?
57. Какие рекомендации по повышению безопасности можно дать?
58. Какие перспективы развития протоколов туннелирования существуют?
59. Как квантовые вычисления повлияют на криптографию туннелирования?
60. Какие стандарты безопасности применяются к протоколам туннелирования?

ФИШИНГ 1.3

1. Введение в фишинг
1.1. Определение фишинга.
1.2. Антология развития фишинга
2. Виды фишинга
2.1. Email-фишинг.
Общая статистика и тенденции
Использование искусственного интеллекта
Популярные методы и примеры атак
2.2. Spear-фишинг.
Примеры реализаций успешных атак
Статистика и последствия атак
Рекомендации по защите от spear-фишинга
2.3. Whaling.
Сценарий whiling-атак

Примеры реализации успешных атак
Противодействие whiling-атакам
2.4. SMS-фишинг (Smishing.
2.5. Веб-фишинг.
3. Методы защиты от фишинга
3.1. Образование и осведомленность.
3.2. Технические меры использования антивирусов и фильтров.
Эффективность применения антивирусов
Ложные срабатывания антивирусов
Рекомендации по выбору антивируса
Использование фильтров электронной почты
3.3. Как распознавать подозрительные ссылки и источники сообщений.
Основные рекомендации по проверке ссылок
Средства проверки безопасности ссылки
3.4. Двухфакторная аутентификация.
Рынок двухфакторной аутентификации
Примеры успешного применения двухфакторной аунтификации(2FA)
4. Последствия фишинга
4.1. Влияние фишинга на личные и корпоративные финансы.
4.2. Ущерб репутации для компаний и организаций.
Потеря доверия клиентов
Финансовые потери
Общественная реакция и юридические обязательства
Текущие тенденции фишинга
Примеры потери репутации
4.3. Правовые аспекты фишинга.
5. Примеры успешных реализаций атак фишинга
5.1. Известные случаи реальных атак и их последствий.
Целевые группы и методы фишинга
Статистика и факты
Телефонное мошенничество
Увеличение количества вредоносных ссылок
5.2. Уроки, извлеченные из атак.
Использование искусственного интеллекта для анализа угроз
Регулярное обучение сотрудников
Интеграция модели Zero Trust(нулевое доверие)
Защита мессенджеров
Обнаружение deepfake
Использование блокчейн-технологий
6. Будущее применение фишинга
6.1. Тенденции и новые технологии.
Основные тенденции развития фишинга
Прогнозы по мошенничеству
Новые технологии в борьбе с фишингом
6.2. Роль искусственного интеллекта в реализации фишинговых атак.

1. Что такое фишинг?
2. Какие методы используют злоумышленники в фишинговых атаках?
3. Как развивался фишинг исторически?
4. Какие современные тенденции наблюдаются в фишинге?
5. Как искусственный интеллект используется в фишинговых атаках?
6. Что такое Email-фишинг?
7. Какая статистика фишинговых атак за 2024 год?
8. Какие методы Email-фишинга наиболее распространены?

9. Что такое Spear-фишинг?
10. Какие примеры успешных Spear-фишинговых атак известны?
11. Какова статистика и последствия Spear-фишинга?
12. Как защититься от Spear-фишинга?
13. Что такое Whaling?
14. Каков типичный сценарий Whaling-атаки?
15. Какие примеры Whaling-атак известны?
16. Как противодействовать Whaling-атакам?
17. Что такое SMS-фишинг (Smishing)?
18. Какие примеры Smishing-атак известны?
19. Как защититься от Smishing?
20. Что такое веб-фишинг?
21. Что такое Browser-in-the-Browser (BiTB) атака?
22. Как QR-коды используются в фишинге?
23. Что такое Phishing-as-a-Service?
24. Как образование помогает в защите от фишинга?
25. Какие программы обучения кибербезопасности существуют?
26. Какие технические меры защиты от фишинга существуют?
27. Как оценивается эффективность антивирусов?
28. Какие антивирусы показывают лучшие результаты?
29. Что такое ложные срабатывания антивирусов?
30. Какие рекомендации по выбору антивируса существуют?
31. Как работают фильтры электронной почты?
32. Как распознавать подозрительные ссылки?
33. Какие средства проверки безопасности ссылок существуют?
34. Что такое двухфакторная аутентификация?
35. Какие тенденции на рынке двухфакторной аутентификации?
36. Какие примеры успешного применения 2FA известны?
37. Как фишинг влияет на личные финансы?
38. Как фишинг влияет на корпоративные финансы?
39. Какой ущерб репутации наносит фишинг компаниям?
40. Как фишинг приводит к потере доверия клиентов?
41. Какие общественные и юридические последствия фишинга?
42. Какие текущие тенденции фишинга наблюдаются?
43. Какие примеры потери репутации из-за фишинга известны?
44. Какие правовые аспекты фишинга существуют?
45. Какое законодательство регулирует ответственность за фишинг?
46. Какие известные случаи фишинговых атак можно привести?
47. Какие целевые группы наиболее уязвимы к фишингу?
48. Какая статистика телефонного мошенничества?
49. Как увеличилось количество вредоносных ссылок?
50. Какие уроки можно извлечь из фишинговых атак?
51. Как использовать ИИ для анализа угроз?
52. Почему важно регулярное обучение сотрудников?
53. Что такое модель Zero Trust?
54. Как защитить мессенджеры от фишинга?
55. Как обнаруживать deepfake?
56. Как блокчейн может помочь в борьбе с фишингом?
57. Какие тенденции развития фишинга ожидаются?
58. Какие прогнозы по мошенничеству на ближайшие годы?
59. Какие новые технологии в борьбе с фишингом появляются?
60. Какова роль ИИ в реализации и защите от фишинговых атак?

ЧЕЛОВЕК ПОСЕРЕДИНЕ 1.3

1.1. Что такое атака “человек посередине” (Man-in-the-Middle, MITM).

1.2. Актуальность проблемы атак MITM в современном мире
Примеры реализации атак “человека посередине”
Последствия атак MITM
Для бизнеса:
Для пользователей:
2. Механизм реализации атаки “человек посередине”
2.1. Этапы реализации атаки.
Перехват данных
Модификация данных
Подмена данных
2.2. Типы атак MITM
Пассивные атаки
Активные атаки
Примеры реализации атак
2.3. Сценарии реализации атак
Атаки на Wi-Fi сети
Атаки на HTTPS
Атаки на VPN
3. Методы защиты от атак “человек посередине”
3.1. Криптографические методы
Шифрование
Цифровая подпись
Обмен ключами
Методы защиты от MITM-атак
Преимущества использования VPN
Рейтинг VPN-сервисов по безопасности и скорости
3.3. Проверка целостности данных и аутентификации.
Методы проверки целостности данных
Методы аутентификации и управления доступом
3.4. Практические рекомендации повышения защищённости
Использование сильных паролей
Обновление программного обеспечения
Бдительность при подключении к сетям Wi-Fi
4. Инструменты обнаружения и предотвращения MITM атак
4.1. Системы обнаружения вторжений (IDS).
Основные типы IDS
Тенденции в IDS
4.2. Системы предотвращения вторжений (IPS).
Интеграция искусственного интеллекта
Методы предотвращения угроз
Различия между IPS и IDS
Проверочные индикаторы ИПС
Будущие тренды
4.3. Программное обеспечение для анализа сетевого трафика.
Основные направления и технологии
Тенденции и изменения
Прогнозы и статистика
4.4. Примеры бесплатных и коммерческих решений.
Бесплатные решения:
Коммерческие решения:

1. Что такое атака «человек посередине» (MITM)?
2. Каков масштаб угрозы MITM-атак?
3. Какие примеры крупных MITM-атак известны?

4. Каковы последствия успешных MITM-атак?
5. Как MITM-атаки влияют на конфиденциальность данных?
6. Что такое ARP-спуфинг в контексте MITM?
7. Как работает DNS-спуфинг?
8. Что такое SSL-стриппинг?
9. Что такое Rogue Access Point?
10. Какие индикаторы указывают на MITM-атаку?
11. Какие последствия для жертв имеют MITM-атаки?
12. Как MITM-атаки влияют на репутацию организаций?
13. Какой ущерб нанесла MITM-атака на бангладешский банк?
14. Как утечка Equifax связана с MITM?
15. Какие уязвимости Wi-Fi позволяют проводить MITM-атаки?
16. Как защитить Wi-Fi-сети от перехвата?
17. Как HTTPS защищает от MITM?
18. Какие уязвимости SSL/TLS существуют?
19. Как VPN защищает от MITM?
20. Какие VPN-протоколы наиболее безопасны?
21. Как шифрование данных защищает от MITM?
22. Какие современные методы шифрования используются?
23. Какие алгоритмы обмена ключами защищают от MITM?
24. Какие практические рекомендации по защите от MITM существуют?
25. Как VPN помогает предотвратить MITM?
26. Какие VPN-сервисы рекомендуются?
27. Как целостность данных защищает от MITM?
28. Какие практики хранения данных рекомендуются?
29. Какие методы контроля доступа предотвращают MITM?
30. Как MFA защищает от MITM?
31. Как обучение пользователей помогает предотвратить MITM?
32. Какие рекомендации по безопасности паролей существуют?
33. Как безопасно использовать публичные Wi-Fi?
34. Что такое IDS и как она обнаруживает MITM?
35. Какие тренды в развитии IDS существуют?
36. Как AI и ML улучшают IDS?
37. Что такое UEBA?
38. Какие вызовы и возможности IDS/IPS существуют?
39. Что такое IPS и чем она отличается от IDS?
40. Какие типы IPS существуют?
41. Какие преимущества имеют современные IPS?
42. Как интегрировать IPS в SOC?
43. Какие программные средства защиты от MITM существуют?
44. Как работает Palo Alto Networks для защиты от MITM?
45. Как Cisco Umbrella защищает от MITM?
46. Какие бесплатные инструменты для защиты от MITM существуют?
47. Как Wireshark помогает обнаружить MITM?
48. Как Let's Encrypt повышает безопасность?
49. Какие перспективы развития защиты от MITM существуют?
50. Как IoT влияет на угрозу MITM?
51. Какие новые технологии появляются для защиты от MITM?
52. Как Zero Trust архитектура защищает от MITM?
53. Какие метрики оценивают эффективность защиты от MITM?
54. Какие правовые аспекты связаны с MITM-атаками?
55. Какие стандарты безопасности помогают предотвратить MITM?
56. Как реагировать на обнаружение MITM-атаки?
57. Какие организационные меры предотвращают MITM?
58. Как аудит безопасности помогает выявить уязвимости к MITM?
59. Какие рекомендации по защите корпоративных сетей от MITM существуют?

60. Какие тенденции развития MITM-атак ожидаются?

ШПИОНСКИЕ ПРОГРАММЫ 1.3

1.1. Классификация шпиопнских программ.
1.2. Распространение шпионских программ и их влияние на безопасность данных.
2. Типы шпионских программ
2.1. Кейлоггеры.
2.2. Spyware.
2.3. Программы-вымогатели (Ransomware).
2.4. Adware.
2.5. Разновидности шпионских троянов, используемые уловки и способы проникновения.
3. Методы распространения шпионских программ
3.1. Зараженные сайты и ссылки.
3.2. Зараженные файлы.
3.3. Социальная инженерия.
3.4. Уязвимости программного обеспечения.
4. Методы обнаружения и защиты от шпионских программ
4.1. Антивирусные программы.
4.2. Фаерволлы.
4.3. Меры предосторожности.
4.4. Проверка на наличие вредоносного ПО.
Методы проверки на наличие вредоносного ПО.
Инструменты проверки.
5. Правовые аспекты
5.1. Законодательство о шпионских программах.
5.2. Защита персональных данных.

1. Что такое шпионские программы (spyware)?
2. Какие типы шпионских программ существуют?
3. Что такое кейлоггеры (keyloggers)?
4. Какие известные примеры кейлоггеров существуют?
5. Что такое Information Stealers?
6. Какова актуальность угрозы шпионских программ?
7. Какие крупные утечки данных связаны со spyware?
8. Какие APT-группировки используют шпионское ПО?
9. Как работают программы для мониторинга устройств?
10. Какие функции имеют популярные spyware-приложения?
11. Как spyware перехватывает сообщения?
12. Как spyware отслеживает геолокацию?
13. Какие функции записи имеют spyware?
14. Как spyware получает доступ к мультимедиа?
15. Какие правовые и этические вопросы связаны с stalkerware?
16. Что такое ransomware и как оно связано со spyware?
17. Какая статистика ransomware-атак за 2024 год?
18. Что такое RAT (Remote Access Trojan)?
19. Какие примеры популярных RAT существуют?
20. Как защититься от ransomware?
21. Что такое adware?
22. Чем adware отличается от spyware?
23. Какие примеры adware существуют?
24. Какие риски создает adware?
25. Какие типы троянских программ существуют?
26. Что такое Trojan-Banker?

27. Что такое Trojan-Downloader?
28. Как трояны распространяются через SFX-архивы?
29. Какие известные трояны можно привести в пример?
30. Как работает Emotet?
31. Какие методы распространения spyware существуют?
32. Как вредоносные вложения используются для распространения?
33. Как поддельные веб-сайты распространяют spyware?
34. Как злоумышленники используют социальную инженерию?
35. Какие типы вредоносных файлов наиболее опасны?
36. Как распознать фишинговое письмо?
37. Какая статистика фишинговых атак существует?
38. Какие методы обнаружения spyware существуют?
39. Как антивирусы обнаруживают spyware?
40. Какие антивирусы эффективны против spyware?
41. Как работает Norton?
42. Как работает Malwarebytes?
43. Как файерволы защищают от spyware?
44. Какие типы файерволов существуют?
45. Как VPN защищает от spyware?
46. Какие методы удаления spyware существуют?
47. Какие правовые аспекты использования spyware существуют?
48. Какая ответственность предусмотрена по статье 273 УК РФ?
49. Какие международные законы регулируют использование spyware?
50. Как CFAA регулирует компьютерные преступления?
51. Какие этические вопросы связаны со spyware?
52. Как spyware влияет на конфиденциальность?
53. Какие рекомендации по защите от spyware существуют?
54. Как обучение пользователей помогает предотвратить заражение?
55. Какие признаки заражения spyware существуют?
56. Как мониторинг системы помогает обнаружить spyware?
57. Какие тенденции развития spyware ожидаются?
58. Как AI влияет на развитие spyware?
59. Какие новые методы защиты от spyware появляются?
60. Какие выводы можно сделать о защите от spyware?

7.2.6 Методика выставления оценки при проведении промежуточной аттестации

(Например: Зачет проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.
2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов
3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.
4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Учебный стандарт и план специальности в условиях цифровой трансформации и сетевой организации пространства	ПК-9.2, ПК-9.3	Тест
2	Проблема обеспечения безопасности автоматизированной информационной системы и сети	ПК-9.3	Тест
3	Модели атакуемых автоматизированных сетей	ПК-9.2	Тест
4	Эпидемические модели автоматизированных сетей	ПК-9.2	Тест
5	Информационная безопасность и социальная инженерия в автоматизированных сетях	ПК-9.2	Тест
6	Автоматизированные сети и деструктивный контент	ПК-9.2	Тест
7	Мониторинг безопасности автоматизированных сетей	ПК-9.2	Тест
8	Перспективы цифровой трансформации и обеспечения безопасности автоматизированных сетей и систем на основе средств искусственного интеллекта	ПК-9.3	Тест
9	Картографирование защищаемого кибер-сетевого пространства	ПК-9.3	Тест
10	Особенности обеспечения безопасности интернета вещей	ПК-9.3	Тест
11	Результаты и перспективы реализации проекта «Безопасный интернет»	ПК-9.3	Тест
12	Риск-мониторинг Интернет-ресурса	ПК-9.3	Тест

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсового проекта осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

№ п/п	Авторы, составители	Заглавие	Годы издания, вид издания
8.1.1.1	А.Г. Остапенко, Н.М. Радько, А.О. Калашников, О.А. Остапенко, Р.К. Бабаджанов	Теория сетевых войн: Эпидемии в телекоммуникационных сетях	2018, печат.
8.1.1.2	А.Г. Остапенко, Д.Г. Плотников, В.Б. Щербаков, А.О. Калашников, О.А. Остапенко	Теория сетевых войн: Атакуемые взвешенные сети	2018, печат.
8.1.1.3	А.Г. Остапенко, А.В. Паринов, А.О. Калашников, В.Б. Щербаков, А.А. Остапенко	Теория сетевых войн: социальные сети и деструктивный контент	2018, печат.
8.1.1.4	А.Г. Остапенко, Е.Ю. Чапурин, А.О. Калашников, О.А. Остапенко, Г.А. Остапенко	Теория сетевых войн: Социальные сети и риск-мониторинг	2019, печат.
8.1.1.5	А.Г. Остапенко Е.Б. Белов, А.О. Калашников, В.П. Лось, О.А. Остапенко	Теория сетевых войн: Социальные сети и психологическая безопасность	2020, печат.
8.1.1.6	А.Г. Остапенко, Е.Б. Белов, А.О. Калашников, В.П. Лось, А.А. Остапенко	Теория сетевых войн: Сетевая эпидемиология	2021, печат
8.1.1.7	А.Г. Остапенко, О.А. Остапенко, Н.М. Лантюхов, И.А. Боков, Д.А. Нархов	Методические указания к курсовым работам по дисциплине «Введение в специальность»	2021, печат

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем

8.2.1 Свидетельство №2017610047 о государственной регистрации программы для ЭВМ и «Netepidemic»

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория 407/5, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

10 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Введение в специальность» читаются лекции, выполняется курсовая работа.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Большое значение по закреплению и совершенствованию знаний имеет самостоятельная работа студентов. Информацию о всех видах самостоятельной работы студенты получают на занятиях.

Методика выполнения курсовой работы изложена в учебно-методическом пособии. Выполнять этапы курсовой работы должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсовой работы, защитой курсовой работы. Освоение дисциплины оценивается на зачете.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад.
Подготовка к дифференцированному зачету	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и решение задач на практических занятиях.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	2	3	4