ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕДЛЬНОЕ УЧРЕЖДЕНИЕ «СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

ЛЕКЦИЯ 1. ТЕМА 1.1. БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

1. Фундаментальные принципы безопасной сети. Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак

Фундаментальные принципы построения безопасной сети базируются на триаде CIA (Confidentiality — конфиденциальность, Integrity — целостность, Availability — доступность). Конфиденциальность достигается применением криптографических механизмов, разграничением доступа и сегментацией сети. Целостность обеспечивается контролем неизменности данных (хеш-суммы, цифровые подписи, контроль версий конфигураций). Доступность поддерживается отказоустойчивыми архитектурами, балансировкой нагрузки, резервированием каналов и планированием восстановления после сбоев.

Современные угрозы сетевой безопасности классифицируются по векторам воздействия:

- **Вредоносное ПО**: вирусы (саморазмножающиеся с внедрением в исполняемые файлы), черви (автономно распространяющиеся по сети), троянские программы (маскируются под легитимный софт).
- **Сетевые атаки**: DDoS (перегрузка ресурсов), MITM (перехват трафика), спуфинг (подмена идентификаторов), сканирование портов для выявления уязвимостей.
- **Атаки на протоколы**: ARP-spoofing, DNS-poisoning, атаки на BGP.
- **Социальная инженерия**: фишинг, вишинг, претекстинг.

Алгоритм действий по минимизации угроз:

1. Провести инвентаризацию активов и классифицировать данные по уровню критичности.
2. Реализовать сегментацию сети (VLAN, микросегментация) с применением принципа наименьших привилегий.
3. Развертывать обновления и патчинг по регламенту (не реже 1 раза в месяц, критические — в течение 72 часов).
4. Внедрить мониторинг аномалий и корреляцию событий (SIEM-системы).
5. Регулярно проводить тестирование на проникновение и анализ уязвимостей (не реже 1 раза в квартал).

2. Безопасность сетевых устройств OSI. Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функций автоматизированной настройки безопасности

Модель OSI позволяет структурировать меры защиты по уровням: физический (контроль доступа к помещениям, кабелям), канальный (защита от ARP-атак, 802.1X), сетевой (ACL, маршрутизация с контролем), транспортный (шифрование TCP-сессий), сеансовый (контроль сессий), представительный (проверка форматов данных), прикладной (защита протоколов HTTP/FTP/SMTP).

Безопасный доступ к сетевым устройствам обеспечивается:

- Использованием SSH вместо Telnet, отключением HTTP-интерфейса.
- Применением строгой аутентификации (многофакторная, сертификаты).
- Ограничением доступа по IP-спискам и временным окнам.

Назначение административных ролей реализуется через RBAC (Role-Based Access Control): администратор, оператор, аудитор, гость — с чётко прописанными правами. Мониторинг и управление выполняются через SNMPv3 (с шифрованием и аутентификацией), NetFlow/IPFIX для анализа трафика, централизованные системы управления конфигурациями (Ansible, Cisco ISE).

Алгоритм настройки безопасного доступа:

1. Отключить Telnet, HTTP, незащищённые протоколы управления.
2. Настроить SSH с ключами и ограничением попыток входа.
3. Создать профили пользователей с ролевой моделью и логированием действий.
4. Настроить SNMPv3 с разделением прав на чтение/запись.
5. Включить NetFlow/sFlow для сбора телеметрии и интеграции с SIEM.

3. Авторизация, аутентификация и учёт доступа (AAA). Свойства AAA. Локальная AAA-аутентификация. Server-based AAA

AAA (Authentication, Authorization, Accounting) — комплекс механизмов контроля доступа. Аутентификация подтверждает личность пользователя, авторизация определяет разрешённые действия, учёт фиксирует события для аудита.

Свойства AAA:

- Масштабируемость (поддержка тысяч пользователей).
- Централизация управления (единая база пользователей).
- Аудит и отчётность (логирование времени, ресурсов, команд).
- Гибкость политик (условия доступа по времени, месту, устройству).

Локальная AAA-аутентификация применяется в небольших сетях: учётные записи хранятся на самом устройстве, пароли хешируются. Server-based AAA использует внешние серверы: RADIUS (для сетевого доступа), TACACS+ (для детального контроля команд на сетевых устройствах), LDAP/Active Directory (для интеграции с корпоративными каталогами).

Алгоритм внедрения AAA:

1. Выбрать протокол (TACACS+ для сетевого оборудования, RADIUS для Wi-Fi и VPN).
2. Развернуть сервер AAA (Cisco ISE, FreeRADIUS) и настроить группы пользователей.
3. Настроить устройства на использование внешнего сервера, отключить локальные учётные записи.
4. Протестировать сценарии входа, отказа, блокировки после нескольких неудачных попыток.
5. Настроить экспорт логов в SIEM для корреляции событий.

4. Реализация технологий брандмауэра ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах

ACL (Access Control List) — списки контроля доступа, фильтрующие трафик по IP-адресам, портам, протоколам. Стандартные ACL фильтруют по источнику, расширенные — по источнику, назначению, протоколу и портам.

Технология брандмауэров включает:

- Пакетные фильтры (на сетевом уровне).
- Межсетевые экраны с отслеживанием состояния (Stateful Inspection).
- Прокси-брандмауэры (на прикладном уровне).

CBAC (Context-Based Access Control) анализирует состояние соединений и динамически открывает обратные порты для сессий. Политики на основе зон (ZBFW — Zone-Based Firewall) группируют интерфейсы по зонам доверия (Inside, DMZ, Outside) и определяют правила перехода между зонами.

Алгоритм реализации ZBFW:

1. Определить зоны безопасности и назначить интерфейсы.
2. Создать пары зон и политики с указанием разрешённого трафика.
3. Настроить классы трафика (class-map) и политики (policy-map).

4. Применить политики к парам зон.
5. Протестировать правила и собрать статистику для оптимизации.

5. Реализация технологий предотвращения вторжения. IPS-технологии. IPS-сигнатуры. Реализация IPS. Проверка и мониторинг IPS

IPS (Intrusion Prevention System) обнаруживает и блокирует атаки в реальном времени. Технологии IPS включают сигнатурный анализ (поиск известных шаблонов атак) и анализ аномалий (выявление отклонений от нормального поведения).

IPS-сигнатуры — это правила, описывающие признаки атак: сигнатуры могут быть сетевыми (для трафика) и хостовыми (для событий на узлах). Реализация IPS выполняется на специализированных сенсорах, в составе NGFW или в виде виртуальных модулей.

Проверка и мониторинг IPS включают:

- Регулярное обновление сигнатур (ежедневно или по расписанию).
- Анализ ложных срабатываний и тонкую настройку правил.
- Интеграцию с SIEM для корреляции событий и приоритизации инцидентов.

Алгоритм развёртывания IPS:

1. Определить точки установки сенсоров (на периметре, внутри сети, на сегментах с критичными данными).
2. Выбрать режим работы: inline (блокировка) или promiscuous (только обнаружение).
3. Импортировать и активировать сигнатуры, отключить неиспользуемые.
4. Настроить пороги срабатывания и исключения для легитимного трафика.
5. Организовать мониторинг событий, отчётность и реагирование на инциденты.

6. Безопасность локальной сети. Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN

Безопасность локальной сети охватывает защиту конечных точек, сегментов и сервисов. Пользовательские компьютеры защищаются антивирусами, EDR-решениями, шифрованием дисков и контролем запуска приложений.

На Layer-2 применяются:

- Port Security (ограничение MAC-адресов на порту).
- DHCP Snooping (защита от поддельных DHCP-серверов).
- Dynamic ARP Inspection (DAIP) против ARP-спуфинга.
- 802.1X для аутентификации устройств при подключении к портам.

Конфигурация безопасности Layer-2 включает активацию этих функций на коммутаторах, ограничение количества MAC-адресов, привязку IP-MAC-порт.

Безопасность беспроводных сетей достигается WPA3, сегментацией гостевого Wi-Fi, отключением WPS, мониторингом Rogue AP. VoIP защищается шифрованием медиа-трафика (SRTP), разделением голосового трафика в отдельный VLAN, аутентификацией SIP-сессий. SAN (Storage Area Network) защищается зонированием, маскированием LUN, шифрованием данных и контролем доступа по WWN.

Алгоритм обеспечения безопасности LAN:

1. Сегментировать сеть по функциональным зонам и применить VLAN.
2. Активировать Port Security, DHCP Snooping, DAI на коммутаторах.
3. Внедрить 802.1X для контроля доступа к проводной сети.
4. Защитить Wi-Fi (WPA3, гостевой сегмент, мониторинг Rogue AP).
5. Настроить защиту VoIP и SAN согласно отраслевым рекомендациям.

7. Криптографические системы. Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей

Криптографические системы обеспечивают конфиденциальность (шифрование), целостность (хеширование, MAC), аутентичность (цифровые подписи, сертификаты). Криптографические сервисы включают TLS/SSL для веб-трафика, IPsec для VPN, S/MIME для почты, SSH для удалённого доступа.

Базовая целостность проверяется с помощью хеш-функций (SHA-256, SHA-3), аутентичность — через цифровые подписи и сертификаты X.509. Конфиденциальность достигается симметричным шифрованием (AES-256) для данных и асимметричным (RSA, ECC) для обмена ключами.

Криптография с открытыми ключами использует пару ключей: публичный для шифрования/проверки подписи, приватный — для расшифровки/создания подписи. Инфраструктура открытых ключей (PKI) управляет выпуском, отзывом и хранением сертификатов.

Алгоритм внедрения PKI:

1. Определить требования к сертификатам (срок действия, назначение).
2. Развернуться удостоверяющий центр (CA) или использовать публичный CA.
3. Выпустить сертификаты для серверов, устройств, пользователей.
4. Настроить валидацию сертификатов на клиентах и серверах.
5. Реализовать процесс отзыва (CRL, OCSP) и ротацию ключей.

8. Реализация технологий VPN. VPN. GRE VPN. Компоненты и функционирование IPsec VPN. Реализация Site-to-site IPsec VPN с использованием CLI. Реализация Site-to-site IPsec VPN с использованием CCP. Реализация Remote-access VPN

VPN (Virtual Private Network) обеспечивает защищённый туннель поверх публичной сети. GRE (Generic Routing Encapsulation) инкапсулирует пакеты, но не шифрует; часто используется вместе с IPsec для защиты.

IPsec VPN включает:

- AH (Authentication Header) для целостности и аутентификации.
- ESP (Encapsulating Security Payload) для конфиденциальности и целостности.
- IKE (Internet Key Exchange) для согласования ключей и параметров.

Компоненты IPsec: SA (Security Association), политики, алгоритмы шифрования и хеширования.

Реализация Site-to-Site IPsec VPN через CLI включает настройку IKE, криптографических карт, ACL для трафика. Через CCP (Cisco Configuration Professional) — графический мастер настройки с выбором параметров и проверкой конфигурации. Remote-access VPN (SSL/IPsec) предоставляет защищённый доступ пользователям с мобильных устройств и ноутбуков.

Алгоритм настройки Site-to-Site IPsec VPN (CLI):

1. Настроить IKE Phase 1 (алгоритмы, время жизни SA, pre-shared key или сертификаты).
2. Определить трафик для шифрования через ACL.
3. Настроить IPsec Phase 2 (трансформационный набор, привязка к ACL).
4. Привязать криптографическую карту к внешнему интерфейсу.
5. Проверить состояние туннеля (show crypto ipsec sa) и трафик.

9. Управление безопасной сетью. Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности

Принципы безопасного дизайна: минимизация поверхности атаки, эшелонированная защита, принцип наименьших привилегий, отказоустойчивость. Безопасная архитектура включает DMZ, сегменты критичных данных, выделенные сети управления.

Управление процессами реализуется через ITIL/COBIT, управление конфигурациями, изменениями и инцидентами. Тестирование на уязвимости проводится с помощью сканеров (Nessus, OpenVAS) и пентестов.

Непрерывность бизнеса обеспечивается планом DRP (Disaster Recovery Plan) с RTO/RPO, резервным ЦОД, репликацией данных. Жизненный цикл сети включает этапы: планирование, проектирование, внедрение, эксплуатация, оптимизация, вывод из эксплуатации.

Регламенты и политики безопасности описывают правила доступа, парольную политику, допустимое использование, порядок реагирования на инциденты.

Алгоритм разработки политик безопасности:

1. Провести аудит текущего состояния и выявить риски.
2. Сформировать рабочую группу с участием ИТ, ИБ, юристов.
3. Определить категории данных и уровни доступа.
4. Написать политики (парольная, гостевого доступа, BYOD и др.).
5. Утвердить, опубликовать, обучить сотрудников, контролировать выполнение.

10. Cisco ASA. Введение в адаптивное устройство безопасности ASA. Конфигурация фаервола на базе ASA с использованием графического интерфейса ASDM. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM

Cisco ASA (Adaptive Security Appliance) — многофункциональное устройство безопасности, объединяющее фаервол, VPN, IPS, URL-фильтрацию. ASDM (Adaptive Security Device Manager) — графический интерфейс для настройки ASA.

Конфигурация фаервола в ASDM включает создание объектов (сети, сервисы), правил доступа (ACL), NAT, политик безопасности. Конфигурация VPN (Site-to-Site, Remote-Access) выполняется через мастера настройки, где задаются параметры IKE, IPsec, группы пользователей, пулы адресов.

Алгоритм базовой настройки ASA через ASDM:

1. Подключиться к ASA через HTTPS и запустить ASDM.
2. Настроить интерфейсы, VLAN, IP-адреса и зоны безопасности.
3. Создать объекты (сети, сервисы) и правила ACL.
4. Настроить NAT (Static/Dynamic) и сервисы (DNS, NTP).
5. Протестировать доступ и собрать статистику.

Алгоритм настройки VPN в ASDM:

1. Запустить мастер Site-to-Site или Remote-Access VPN.
2. Указать параметры IKE (алгоритмы, pre-shared key/сертификаты).
3. Задать локальные и удалённые сети, пул адресов.
4. Настроить группы пользователей и политики шифрования.
5. Проверить статус туннеля и трафик.