ЧПОУ "СККИТ"

Безопасность компьютерных систем

10 модулей: от принципов безопасной сети и современных угроз до Cisco ASA, IPS, VPN и криптографии — для специалистов по сетевой безопасности.

ПОВЕСТКА КУРСА

Содержание: 10 модулей курса

От принципов и угроз — через AAA, брандмауэры, IPS и криптографию — к VPN, управлению сетью и Cisco ASA.

01	**Принципы и угрозы**	Безопасная сеть, вирусы, черви, трояны, методы атак
02	**Устройства и OSI, AAA, брандмауэры**	Доступ и роли, локальная и server-based AAA, ACL и CBAC
03	**IPS и безопасность локальной сети**	Сигнатуры и мониторинг; Layer-2, WLAN, VoIP, SAN
04	**Криптография**	Криптосервисы, целостность, конфиденциальность, открытые ключи
05	**VPN и IPSec**	GRE, site-to-site через CLI и CCP, remote-access
06	**Управление безопасной сетью**	Архитектура, тестирование, BCP/DR, политики
07	**Cisco ASA и ASDM**	Настройка фаирвола и VPN через графический интерфейс

МАСШТАБ УГРОЗ

Масштаб угроз в 2026 году

$12 трлн

Ущерб от киберпреступности

Глобальные потери экономики за год

$240 млрд

Расходы на кибербезопасность

Рост на 12,5% год к году

70%+

Проникновений через дипфейки

Доля успешных атак с обманом ИИ

Ransomware: 2 509 подтверждённых инцидентов во II квартале 2026 года и 91 активная группа

Источник: отчёты по кибербезопасности и ransomware, 2026

ПРИНЦИПЫ

Фундаментальные принципы безопасной сети

01

Триада CIA

Конфиденциальность — данные видит только тот, кому положено; целостность — данные не изменены; доступность — сервис работает, когда нужен.

02

Эшелонированная защита (defense-in-depth)

Несколько рубежей: ACL и брандмауэр, IPS, AAA, сегментация, шифрование VPN. Пробить один рубеж недостаточно для компрометации сети.

03

Минимальные привилегии

Пользователь и администратор получают только те права, что нужны для задачи. Административные роли назначаются по зонам ответственности.

04

Разделение зон доверия и «нулевое доверие»

Внутренняя и внешняя сети, DMZ и гостевая сеть разделены политиками. Zero Trust: не доверяем по умолчанию, проверяем каждое подключение.

05

Привязка принципов к уровням OSI

Layer-2 — port-security, VLAN, DHCP snooping; Layer-3/4 — ACL и зоны брандмауэра; Layer-5–7 — IPS-сигнатуры, AAA, криптография и VPN.

УГРОЗЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

Вредоносное ПО и методы атак

01

Вирус

Внедряется в исполняемые файлы и заражает их; для распространения нужно действие пользователя — запуск заражённой программы.

02

Червь

Самовоспроизводится и распространяется по сети без участия человека, эксплуатируя уязвимости протоколов и сервисов.

03

Троянский конь

Маскируется под полезное ПО; не размножается сам, а открывает злоумышленнику скрытый доступ (backdoor) или крадёт данные.

04

Фишинг и социальная инженерия

Обман пользователя через поддельные письма, сайты и звонки ради учётных данных, платежей или запуска вредоносного кода.

05

Атака «человек посередине» (MITM)

Перехват и подмена трафика между сторонами: ARP-спуфинг, поддельные точки доступа, перехват незашифрованных сессий.

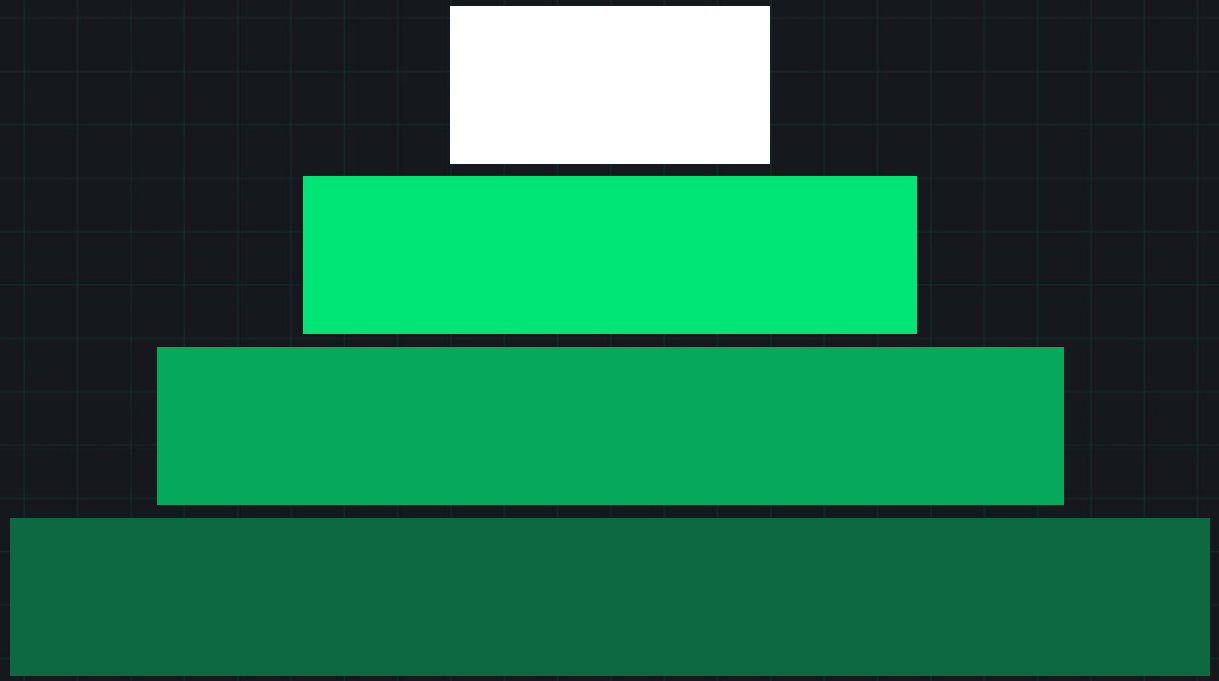
06

DoS/DDoS и SQL-инъекции

Отказ в обслуживании за счёт перегрузки ресурсов; SQL-инъекция — внедрение запроса через ввод формы для доступа к базе данных.

ИЕРАРХИЯ ЗАЩИТЫ

Безопасность сетевых устройств и модель OSI



Управление и мониторинг

Syslog, SNMP, NTP: журналы, опрос состояний, единое время

Административные роли

Разграничение привилегий: уровни 1–15, отдельные учётные записи

Безопасный доступ

Консоль, VTY, SSH вместо Telnet; AAA и таймауты сессий

Автоматизация и OSI

AutoSecure, Cisco SDM/CCP; защита по уровням модели OSI

AAA

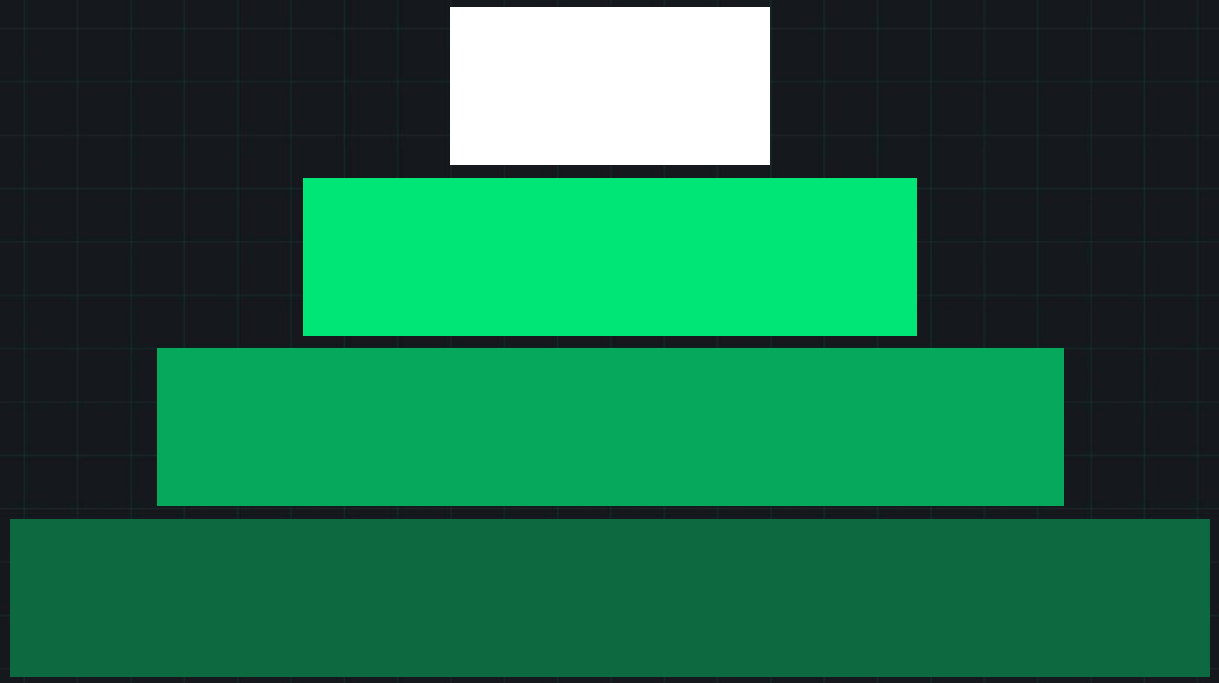
Локальная и серверная аутентификация: что выбрать

Критерий	Локальная AAA	Серверная AAA (TACACS+/RADIUS)
Где хранятся учётные данные	На самом устройстве (username/password)	На центральном сервере
Масштабируемость	Низкая: настройка на каждом устройстве	Высокая: единая база пользователей
Централизация	Нет, политики разрознены	Да, единые политики для всей сети
Учёт действий (Accounting)	Ограниченный, локальные логи	Полный: централизованный сбор и аудит
Управление доступом	Через privilege levels	Через роли и атрибуты на сервере
Отказоустойчивость	Зависит от устройства	Резервные серверы и fallback

Локальная AAA — для малых сетей и резерва; серверная — стандарт масштабируемой инфраструктуры.

БРАНДМАУЭРЫ

Эволюция контроля доступа: от ACL к зонным политикам



Зонные политики (ZBF)

Пары зон inside/outside/DMZ, инспекция на уровне приложений

CBAC

Контекстный контроль: stateful inspection для протоколов

Extended ACL

Фильтрация по IP, портам и протоколам

Standard ACL

Базовый контроль по IP-адресу источника

ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ

IPS: сигнатуры, реализация и мониторинг

1

Сигнатуры и обнаружение

Сигнатурный метод: сенсор сравнивает трафик с базой известных шаблонов атак и срабатывает при совпадении — точно, но требует регулярного обновления баз.

2

Режимы IPS и IDS, размещение сенсора

IDS только фиксирует события, IPS блокирует трафик в реальном времени; сенсор ставится в разрыв (inline) на периметре или в ключевых сегментах сети.

3

Реализация на Cisco IOS IPS

Загрузка и компиляция сигнатур, включение IPS на интерфейсе, выбор категорий и действий (alert, drop, reset) — через CLI или CCP.

4

Проверка и мониторинг

Анализ срабатываний и ложных тревог, журналы и оповещения, тюнинг сигнатур и регулярное обновление баз для снижения шума.

БЕЗОПАСНОСТЬ ЛОКАЛЬНОЙ СЕТИ

Layer-2, WLAN, VoIP и SAN: защита на всех уровнях доступа

Защита конечных устройств

Антивирус, своевременные обновления и host-based firewall на каждом пользовательском ПК

Атаки Layer-2

MAC flooding, ARP spoofing и VLAN hopping обходят обычную сегментацию коммутатора

Контрмеры на коммутаторе

Port security, DHCP snooping, Dynamic ARP Inspection и BPDU Guard

Беспроводные сети

WPA2/WPA3, 802.1X и контроль точек доступа вместо открытых SSID

VoIP

Изоляция голосового трафика в отдельном VLAN и защита сигнализации

SAN

Отдельный защищённый сегмент хранения, зонирование и контроль доступа к массивам

КРИПТОГРАФИЯ

Криптографические системы: сервисы и механизмы

Конфиденциальность

Симметричные шифры AES и DES скрывают содержимое трафика от посторонних

Целостность

Хеши и HMAC фиксируют любое изменение данных при передаче

Аутентичность

Цифровая подпись подтверждает, кто именно отправил сообщение

Открытые ключи

RSA и обмен ключами Диффи–Хеллмана решают задачу распределения ключей

PKI и сертификаты

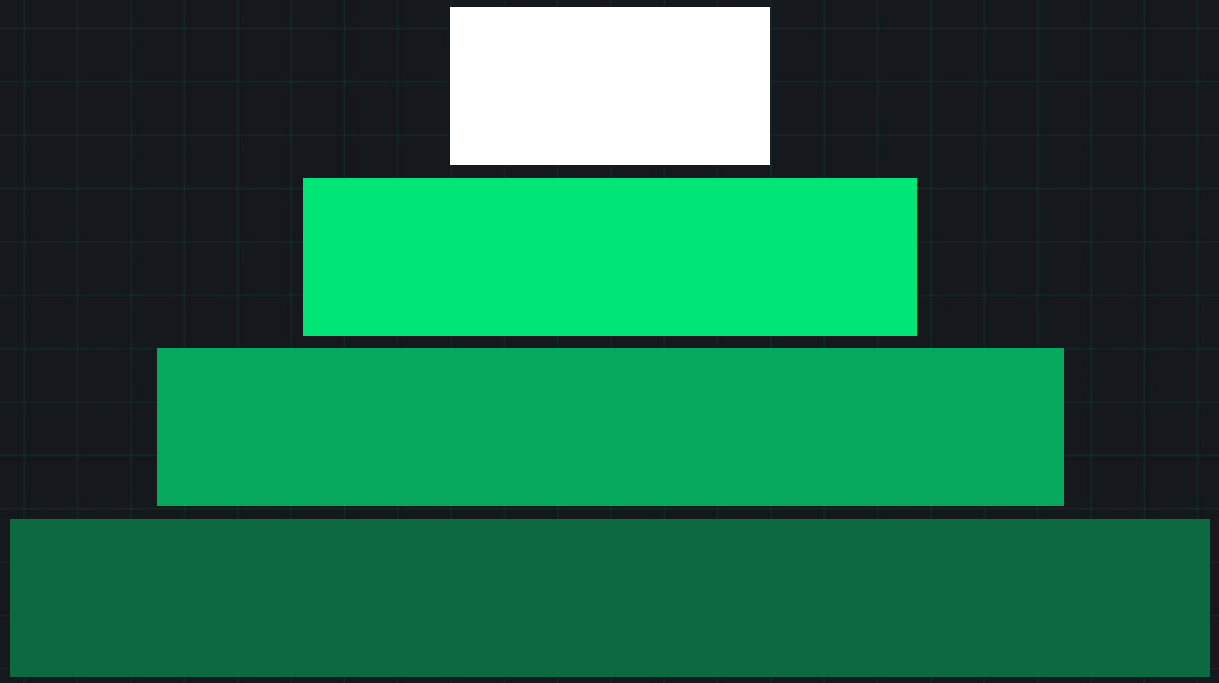
Удостоверяющие центры связывают открытый ключ с личностью владельца

Комбинированная схема

Асимметрика защищает обмен ключом, симметрика шифрует сами данные

VPN И IPSEC

VPN: от GRE-туннеля до IPSec и удалённого доступа



Remote-access VPN

Easy VPN и SSL VPN — защищённый доступ мобильных и домашних сотрудников

IPSec VPN

AH/ESP, transport/tunnel, IKE фазы 1 и 2 — шифрование и аутентичность трафика

Site-to-site IPSec

Постоянные туннели между площадками: настройка через CLI и через CCP

GRE VPN

Простой инкапсулирующий туннель без шифрования — база для маршрутизации и multicast

РАЗДЕЛ 9 · УПРАВЛЕНИЕ БЕЗОПАСНОЙ СЕТЬЮ

Управление безопасной сетью: от политики до восстановления

1

Проектирование и архитектура

Принципы безопасного дизайна: сегментация, минимум привилегий, эшелонированная защита, документированный жизненный цикл сети и единые политики безопасности компании.

2

Процессы, тестирование, BCP/DRP

Управление процессами и политиками, сканирование уязвимостей и пентест, непрерывность бизнеса и план восстановления после аварий с проверкой их работоспособности.

3

Результат: управляемая безопасность

Регламенты и политики превращают разрозненные средства защиты в измеримый, проверяемый и восстанавливаемый контур безопасности сети.

ПРАКТИКА · CISCO ASA

Cisco ASA: настройка через ASDM

1

Подключение и зоны безопасности

ASDM запускается по HTTPS с учётной записью администратора; интерфейсам назначаются зоны (inside, outside, DMZ) и уровни защищённости security level.

2

Брандмауэр: ACL и политики

В ASDM создаются ACL и правила зональных политик: разрешённый трафик из зоны с высоким уровнем в зону с низким, контроль доступа CBAC и NAT.

3

VPN и проверка правил

Мастер VPN в ASDM настраивает site-to-site и remote-access IPSec; затем проверяются правила, журналы и мониторинг соединений.

ФИНАЛ

Спасибо за внимание!

От принципов — к практике: стройте защиту слоями, проверяйте её на стенде и подтверждайте квалификацию.