## 1. Реализация сетевого протокола SSL

* **SSL (Secure Sockets Layer)**, предшественник TLS, обеспечивает защищённое шифрованное соединение между клиентом и сервером.
* Включает **рукопожатие (handshake)**, во время которого выбираются криптографические параметры, происходит аутентификация сервера (иногда клиента) и устанавливается общий ключ.
* Реализация предполагает использование **цифровых сертификатов**, выданных удостоверяющими центрами (CA), и симметричных алгоритмов шифрования для основного трафика.

## 2. Стандарты информационной безопасности

* Ключевые международные стандарты: **серия ISO/IEC 27000**, NIST SP 800, COBIT, PCI DSS (для платёжных карт).
* В России действуют **ГОСТ**-стандарты, регулирующие криптографию (ГОСТ Р 34.12-2015 «Магма», «Кузнечик»), ЭЦП, а также требования ФСТЭК и ФСБ.
* Цель стандартов: унификация и формализация требований, процедур и методов защиты информации.

## 3. Методы обеспечения безопасности информационных систем

* **Организационные** (политики, регламенты, обучение персонала).
* **Технические** (межсетевые экраны, IDS/IPS, антивирусы, шифрование).
* **Криптографические** (конфиденциальность, целостность, аутентификация, ЭЦП).
* **Процессные** (аудит, мониторинг, тесты на проникновение).

## 4. Основные атаки и угрозы информационным системам

* **Зловредное ПО** (вирусы, трояны, рансомваре).
* **Сетевые атаки** (DDoS, фишинг, MITM, SQL-инъекции, XSS).
* **Социальная инженерия** (обман, фишинг-письма).
* **Внутренние угрозы** (недобросовестные сотрудники, ошибки администраторов).

## 5. Модель предполагаемого противника

* Описание типа, ресурсов, мотивации и возможностей злоумышленника.
* Модель учитывает: **уровень квалификации**, финансовые ресурсы, доступ к эксплойтам, инсайдерские данные.
* Основывается на оценке **рисков** и помогает определить соответствующие меры защиты.

## 6. Внешний периметр, зоны безопасности, контуры защиты, контролируемая зона

* **Внешний периметр** — граница между корпоративной сетью и внешними сетями (Интернет).
* **Зоны безопасности** — сегменты сети с разным уровнем доверия (DMZ, внутренняя сеть и т.д.).
* **Контуры защиты** — уровни (слои) технических и организационных мер, защищающих зоны.
* **Контролируемая зона** — физическая территория или сетевой сегмент, где организация может обеспечить полный контроль.

## 7. Политики безопасности

* Набор формализованных правил и требований, определяющих, как защищается информация в организации.
* Включают политики паролей, резервного копирования, обновлений, управления доступом, реагирования на инциденты.
* Регламентируют **роли и обязанности** персонала, порядок изменения конфигураций и ведения аудита.

## 8. Модель системы защиты

* Определяет архитектуру и принципы реализации ИБ (многоуровневая модель, модель с зонами безопасности, контроль доступа, криптография и т.д.).
* Может опираться на формальные модели (Белла–Лападулы, Биба, Кларка–Вилсона) или на практические стандарты (ISO 27001).
* Цель — обеспечить согласованную защиту **конфиденциальности, целостности и доступности**.

## 9. Специализированные аппаратно-программные системы защиты безопасности

* Устройства и решения «всё в одном» (UTM — Unified Threat Management), HSM (Hardware Security Module), VPN-шлюзы, средства защиты каналов связи.
* Гарантируют высокую производительность и защищённость ключевых операций (например, генерацию, хранение и управление ключами).
* Сертифицируются регулирующими органами (ФСТЭК, ФСБ) для использования в государственных и коммерческих системах.

## 10. Системы безопасности «Криптоцентр»

* Отечественный программно-аппаратный комплекс для **защиты каналов связи**, организации VPN, управления ключами и сертификатами.
* Может обеспечивать шифрование на уровне IPsec, SSL/TLS, использовать ГОСТ-алгоритмы.
* Предоставляет централизованное администрирование и мониторинг.

## 11. Системы безопасности «Криптон»

* Семейство решений (например, «Криптон-Endpoint» и др.), предназначенных для защиты рабочих станций, серверов, сетевых коммуникаций.
* Как правило, включает **криптографические модули** (ГОСТ) для шифрования каналов и хранения ключей.
* Может также обеспечивать контроль целостности, управление доступом.

## 12. Системы безопасности «Верба»

* Линейка отечественных средств шифрования голоса, данных и IP-трафика (Voice/IP).
* Часто применяется в государственных структурах, силовых ведомствах, обеспечивая безопасную связь.
* Поддерживает механизмы **ГОСТ-шифрования** и сертифицирована в ФСБ/ФСТЭК.

## 13. Системы безопасности «Крипто-Про»

* Популярный в РФ **криптопровайдер** и инструменты для реализации ЭЦП, шифрования, криптографической защиты на рабочих станциях и серверах.
* Участвует в инфраструктуре открытых ключей (PKI), обеспечивает поддержку ГОСТ-алгоритмов и совместимость с программными продуктами (например, 1С, Microsoft).
* Используется для формирования, проверки и управления **квалифицированными сертификатами**.

## 14. Биометрические системы

* Системы аутентификации по **физиологическим** (отпечаток пальца, радужка глаза, лицо) или **поведенческим** (голос, подпись) характеристикам.
* Достоинства: повышенная надёжность (сложнее подделать), удобство для пользователей.
* Недостатки: риск утечки биометрических шаблонов, сложность корректного хранения, возможность ложных срабатываний.

## 15. Правовые аспекты цифровой подписи

* В РФ регламентируется ФЗ № 63 «Об электронной подписи» — три вида: простая, усиленная неквалифицированная, усиленная квалифицированная.
* В международном контексте — eIDAS (ЕС), UETA, ESIGN (США).
* Цифровая подпись (ЭЦП) обеспечивает **неотказуемость**, целостность и аутентичность документа.

## 16. Интегрированная защита компьютерных сетей

* Комплексный подход: межсетевые экраны, IDS/IPS, антивирус, DLP, VPN, система управления уязвимостями и пр.
* Включает как аппаратные, так и программные средства, а также организационные меры (регламенты, обучение).
* Главная цель — **слоистая (эшелонированная) защита**, охватывающая все уровни: от периметра до рабочих станций.

## 17. Политика безопасности управления компьютерными сетями

* Определяет, кто и как администрирует сеть, какие инструменты и каналы удалённого доступа разрешены.
* Включает требования к **аутентификации** администраторов, ведению журналов изменений, сегментации доступа, резервному копированию настроек.
* Регламентирует доступ к сетевым устройствам (маршрутизаторы, коммутаторы, брандмауэры).

## 18. Защита подсистемы управления компьютерными сетями

* Использование **административных VLAN** (Out-of-Band Management), шифрование управления (SSH вместо Telnet, HTTPS вместо HTTP).
* Контроль привилегированных учётных записей, логирование и аудит действий администраторов.
* Защита от атак на SNMP (использование безопасных версий SNMPv3), фильтрация доступа к портам управления.

## 19. Технологии межсетевых экранов: фильтрация пакетов, применение шлюзов, прочие компоненты брандмауэров

* **Фильтрация пакетов** (Packet Filtering): анализ заголовков IP, портов, протоколов.
* **Межсетевые прокси-шлюзы** (Application Gateway): фильтрация на уровне приложений (HTTP, FTP).
* **Системы stateful inspection**: отслеживают состояния соединений, могут динамически открывать/закрывать порты.
* **UTM** (Unified Threat Management): совмещают firewall, IDS, антивирус, контент-фильтрацию.

## 20. Функции межсетевого экранирования

* Контроль и фильтрация входящего/исходящего трафика.
* Разделение сети на сегменты, предотвращение проникновений извне.
* Логирование и мониторинг сетевых сессий, а также поддержка **VPN** (в некоторых решениях).

## 21. Аппаратные брандмауэры

* Специализированные устройства (Cisco ASA, Fortinet, Check Point и др.) с высокой пропускной способностью и надёжностью.
* Удобны для развертывания на **корпоративном периметре**, имеют аппаратное ускорение криптографии.
* Поддерживают расширенные функции: IDS/IPS, VPN, веб-фильтрация, балансировка нагрузки.

## 22. Политика безопасности межсетевого экрана

* Набор **правил фильтрации** (ACL — Access Control Lists) и политик NAT, определяющих, какой трафик разрешён или запрещён.
* Учитывает IP-адреса, порты, протоколы, время, а также аутентификацию пользователей (в некоторых случаях).
* Включает регулярный аудит и обновление правил, ведение логов, отслеживание аномалий.

## 23. Трансляторы сетевых адресов

* **NAT (Network Address Translation)** позволяет отображать частные IP-адреса во внешний (публичный) IP и обратно.
* Способствует маскировке внутренней топологии сети, улучшает безопасность.
* Варианты: **SNAT** (Source NAT), **DNAT** (Destination NAT), **PAT** (перевод многих внутренних адресов на один публичный с разными портами).

## 24. Шлюзы и прокси-серверы

* **Шлюз** (gateway) — узел, совмещающий разные протоколы или сети (например, VoIP-шлюз, VPN-шлюз).
* **Прокси-сервер** — промежуточный сервер, принимающий запросы клиентов и передающий их от своего имени к целевым ресурсам.
* Прокси обеспечивает **кэширование**, фильтрацию трафика, анонимизацию, может собирать статистику и применять правила контент-фильтрации.

## 25. Распознавание контента и его фильтрация

* Контент-фильтрация (URL-фильтрация, антивирусная проверка, DLP) — анализ содержимого пакетов или файлов.
* Может блокировать нежелательный трафик (порнография, азартные игры, вредоносные сайты) или конфиденциальные данные (номера карт, персональные данные).
* Используются решения: **Blue Coat, WebSense, Kaspersky Secure Web Gateway** и т.д.

## 26. Основы криптографии

* Наука о методах обеспечения **конфиденциальности**, **целостности**, **аутентичности**, **неотказуемости** информации.
* Включает **симметричные алгоритмы шифрования**, **асимметричные алгоритмы**, **хэш-функции**, **ЭЦП**, протоколы обмена ключами.
* Опирается на математические задачи (дискретное логарифмирование, факторизацию и пр.).

## 27. Симметричные и асимметричные алгоритмы шифрования

* **Симметричные** (один ключ для шифрования и расшифрования): AES, ГОСТ, 3DES. Быстрые, но сложность в безопасной передаче ключа.
* **Асимметричные** (пара ключей: открытый и закрытый): RSA, ECC. Проще обмен ключами, но работают медленнее.

## 28. Потоковые и блочные шифры

* **Потоковые**: шифруют данные побитово или побайтово (RC4, A5/1). Удобны для потоковых каналов, но есть риски, связанные с повторным использованием ключевого потока.
* **Блочные**: шифруют данные блоками фиксированного размера (AES — 128-битный блок, ГОСТ Магма — 64-битный блок). Поддерживают разные режимы (ECB, CBC, CTR и т.п.).

## 29. Криптографические генераторы псевдослучайных последовательностей

* **PRNG** (pseudo-random number generator) формируют последовательности, детерминированно зависящие от начального состояния (seed).
* В криптографии используют криптостойкие PRNG (Fortuna, ANSI X9.17, Hash-DRBG, HMAC-DRBG).
* Отличие от **истинной случайности** (TRNG): PRNG повторяем и предсказуем при известном seed.

## 30. Шифр одноразового блокнота

* **One-Time Pad (OTP)**: каждый символ исходного текста складывается по модулю 2 с символом ключа такой же длины.
* При полностью случайном ключе, равном длине сообщения, и единовременном использовании является **абсолютно стойким**.
* Практически сложно обеспечить надёжное хранение и распространение длинных ключей.

## 31. Криптографические протоколы

* Соглашения о формате и порядке взаимодействия, обеспечивающие безопасную передачу данных.
* Примеры: **SSL/TLS**, SSH, IPsec, Kerberos, PGP/OpenPGP.
* Обычно включают механизмы **аутентификации**, **шифрования**, **контроля целостности**.

## 32. Стандарт ANSI X.917

* Старый криптографический стандарт, описывающий метод генерации псевдослучайных чисел на базе блочного шифра (3DES).
* Применяется для ключевых генераторов в финансовых системах.
* Задаёт схему с «Seed Key» и «Seed Value» для формирования выходной последовательности.

## 33. Алгоритм Диффи-Хеллмана

* Позволяет двум сторонам согласовать **общий секретный ключ** по незащищённому каналу.
* Основан на сложности вычисления дискретного логарифма.
* Не обеспечивает аутентификацию сторон по умолчанию.

## 34. Схема Диффи-Хеллмана

1. Выбор общего простого числа p и основания g.
2. Участник A выбирает секрет a, вычисляет A=  mod p. Участник B выбирает b, вычисляет B=  mod p.
3. Обмен публичными значениями A и B.
4. Общий ключ: K=  mod p. Атака MITM возможна без доп. аутентификации.

## 35. MITM-атака на схему Диффи-Хеллмана

* Злоумышленник перехватывает AAA и BBB, подменяет их своими значениями.
* В результате A и B устанавливают ключи с атакующим, а не друг с другом.
* Защита: использовать **цифровые подписи**, сертификаты или иные методы аутентификации.

## 36. Рекурсивный алгоритм Евклида

* Используется для нахождения **наибольшего общего делителя (НОД)** двух чисел.
* Рекурсивная формула: gcd(a,b)=gcd(b,a mod b).
* Важен в криптографии для работы с ключами (RSA), при вычислении обратных элементов по модулю.

## 37. Расширенный алгоритм Евклида

* Не только вычисляет gcd(a,b), но и находит **коэффициенты** x и y такие, что ax+by=gcd.
* Применяется для вычисления **обратного элемента** по модулю (в RSA, Диффи–Хеллмане и т.д.).
* Реализуется и рекурсивно, и итеративно.

## 38. Алгоритм RSA

1. Выбирают два больших простых числа p и q.
2. Вычисляют n=p×q и ϕ(n)=(p−1)(q−1).
3. Выбирают e взаимно простое с ϕ(n).
4. Определяют d (обратное к e по модулю ϕ(n)).
5. Открытый ключ: (e,n). Закрытый ключ: (d,n).

* Используется для шифрования и ЭЦП.

## 39. Атаки и угрозы для хэш-функций, стойкость хэш-функции

* Основные требования стойкости: **невозможность найти исходное сообщение по хэшу** (preimage resistance) и **трудность найти два сообщения с одинаковым хэшем** (collision resistance).
* Атаки: поиск коллизий (метод дня рождения), выборочные коллизии, расширение длины (для некоторых конструкций).
* Примеры: уязвимости в MD5, SHA-1. Современные – SHA-2 (SHA-256, SHA-512) и SHA-3 (Keccak).

## 40. Хэш-функция SHA

* Семейство **Secure Hash Algorithm**: SHA-1 (160 бит), SHA-2 (224/256/384/512 бит), SHA-3.
* Применяются для проверки целостности, хранения паролей (с солью), формирования ЭЦП.
* SHA-1 признан менее надёжным (есть частичный прецедент коллизий), рекомендован переход на SHA-2/3.

## 41. Алгоритмы ЭЦП: RSA, DSA

* **RSA**: подпись формируется возведением хэша сообщения в степень d (закрытый ключ). Проверка — возведение результата в e (открытый ключ).
* **DSA** (Digital Signature Algorithm): основан на сложности дискретного логарифмирования. Подпись формируется через пару (r,s), проверяется уравнением на модуль p.
* Оба алгоритма требуют **надёжных генераторов** случайных чисел, особенно DSA (ранее были уязвимости с повторным k).

## 42. Российский и американский стандарты шифрования (ГОСТ, DES, AES)

* **ГОСТ Р 34.12-2015**: «Магма» (64-бит блок) и «Кузнечик» (128-бит блок), ключ 256 бит.
* **DES** (Data Encryption Standard), устаревший 56-битный ключ, уязвим к перебору.
* **AES** (Advanced Encryption Standard): блочный 128-битный шифр с ключами 128/192/256 бит. Современный стандарт США.

## 43. Сеть Фейстеля

* Конструкция блочного шифра, делит блок на две половины (L, R) и выполняет серию раундов, где одна половина модифицируется на основе функции шифрования от другой половины и ключа.
* Используется в **DES**, **Blowfish**, **Магма**.
* Обеспечивает возможность шифрования/расшифрования с тем же алгоритмом (реверсирование структуры).

## 44. Основные характеристики DES

* Блок 64 бита, ключ 56 бит (на практике 64 бита, но 8 используются для чётности).
* 16 раундов, основанных на **сети Фейстеля**.
* Устаревший по причине малого размера ключа, часто заменяется на 3DES или AES.

## 45. Схема DES: начальная перестановка, раунды

* **Initial Permutation (IP)** — перестановка бит перед началом раундов.
* 16 раундов сети Фейстеля: в каждом формируются подтключи и выполняется функция F (S-блоки, перестановка).
* **Inverse IP** — завершающая перестановка для получения зашифрованного блока.

## 46. Основные характеристики AES

* Блок 128 бит, ключ 128/192/256 бит, разное число раундов (10/12/14).
* Быстрый, эффективен на широком спектре платформ, хорошо исследован на криптостойкость.
* Использует операции над полем GF() (операции «SubBytes», «MixColumns» и т.д.).

## 47. Раунды алгоритма AES: SubBytes, ShiftRows, MixColumns, AddRoundKey

1. **SubBytes** — замена каждого байта по нелинейной S-Box.
2. **ShiftRows** — циклический сдвиг строк в матрице состояния.
3. **MixColumns** — умножение столбцов матрицы состояния в поле GF() (пропускается в последнем раунде).
4. **AddRoundKey** — побитовое XOR состояния с подключом.

## 48. Криптостойкость AES

* При ключе 128 бит полный перебор составляет операций, что пока считается недостижимым.
* Нет практических атак, позволяющих взломать AES быстрее перебора.
* При более длинных ключах (192/256 бит) стойкость ещё выше.

## 49. Алгоритм IDEA

* **International Data Encryption Algorithm**, блок 64 бита, ключ 128 бит.
* Состоит из 8 идентичных раундов и заключительной трансформации, использует **операции модульного умножения**, сложения по модулю и XOR.
* Разработан как замена DES, патент был в Европе и США (срок действия патента истёк).

## 50. Основные характеристики и операции алгоритма IDEA

* Блок: 64 бита, ключ: 128 бит, 8 раундов + выводной раунд.
* Операции в каждом раунде:
  1. Деление блока на 4 части по 16 бит.
  2. Модульное умножение (по ), сложение по модулю , XOR.
  3. Перестановки для следующего шага.
* Обеспечивает хорошую криптостойкость, но менее распространён, чем AES.

## 51. Локальный администратор безопасности

* Специалист/учётная запись с правами на администрирование безопасности в конкретной системе или узле (компьютере).
* Отвечает за установку и настройку программ защиты, управление локальными политиками, мониторинг событий безопасности.
* Может иметь ограниченные полномочия по сравнению с глобальным (доменным) администратором.

## 52. Центр аутентификации

* Служба/компонента, проверяющая подлинность субъектов (пользователей, устройств) при их входе в систему.
* Пример: **Kerberos KDC** (Key Distribution Center), проверяет билеты TGT, выдаёт сервис-билеты.
* Может быть частью инфраструктуры PKI, где используется CA для выпуска сертификатов.

## 53. Диспетчер учетных записей

* Утилита или служба, управляющая созданием, изменением, удалением, блокировкой учётных записей пользователей и групп.
* В Windows это может быть **Local Users and Groups**, в домене – **Active Directory Users and Computers**.
* Обеспечивает безопасность путём настройки паролей, групповых политик, прав и разрешений.

## 54. Монитор безопасности

* ПО или служба, которая **отслеживает события** в системе (журналы, действия пользователей, сетевой трафик), оповещает о подозрительной активности.
* Может быть частью **SIEM** (Security Information and Event Management) — агрегирует и анализирует логи из разных источников.
* Цель: быстрое обнаружение инцидентов, формирование отчётов и алертов.

## 55. Механизмы контроля доступа и аутентификации

* Модели контроля: **DAC** (дискреционная), **MAC** (мандатная), **RBAC** (ролевая), **ABAC** (атрибутивная).
* Методы аутентификации: **по знаниям** (пароль), **по владению** (токен, смарт-карта), **по биометрии**.
* Основные принципы: **минимальные привилегии**, разделение обязанностей, подтверждение личности.

## 56. Слабости парольных протоколов аутентификации

* Угрозы: **брутфорс**, перехват хэша, фишинг.
* Слабые пароли, повторное использование паролей, отсутствие соли при хранении хэшей.
* Меры: многофакторная аутентификация, сложные пароли, защита хранимых хэшей (bcrypt, PBKDF2, Argon2).

## 57. Виды атак и угроз для протоколов аутентификации

* **Перехват сеанса** (session hijacking).
* **Replay-атаки** (повтор ранее перехваченного трафика).
* **MITM** (подмена конечной точки).
* **Phishing** (выманивание паролей).
* Защита: использование TLS, nonce, одноразовых токенов, 2FA.

## 58. Базовые технологии безопасности информационных систем

* **Шифрование** (конфиденциальность), **ЭЦП** (целостность, неотказуемость).
* **Межсетевые экраны** и **IDS/IPS**, антивирусы.
* **Резервное копирование**, **управление доступом** (ACL, RBAC).
* **Аудит, мониторинг**, системное обновление.

## 59. Идентификация, аутентификация и авторизация. Определения, отличия и сходство

* **Идентификация**: субъект сообщает свои данные (логин, ID).
* **Аутентификация**: проверка, действительно ли субъект владеет заявленной идентификацией (пароль, сертификат, биометрия).
* **Авторизация**: предоставление или ограничение прав доступа к ресурсам после успешной аутентификации.
* Все три — части единого процесса контроля доступа.

## 60. Аудит информационной безопасности. Методы проведения аудита информационной безопасности

* **Аудит ИБ** — оценка соответствия системы требованиям (стандартам, политикам, законам).
* Методы: анализ документации, интервью с персоналом, инструментальное тестирование (сканирование уязвимостей, пентесты), наблюдение.
* Результат: отчёт с **выявленными несоответствиями**, рекомендациями по устранению.