Вот развернутые ответы на вопросы к зачету по Основам информационной безопасности, сгруппированные по темам и основанные на предоставленной информации:

1. Информационная безопасность в мире.

- **Актуальность:** Глобальная цифровизация всех сфер жизни, рост числа и сложности киберугроз, стремление бизнеса защитить активы, обилие информационных систем, развитие передовых технологий (ИИ) делают ИБ критически важной для всех стран.
- **Подходы:** Различаются по регионам. Преобладает регулирование через законы о защите данных (GDPR в ЕС, CCPA в США, PIPL в Китае) и директивы по кибербезопасности (NIS2 в ЕС).
- **Ключевые проблемы:** Глобальный характер угроз (APT, вредоносное ПО), трансграничные потоки данных, регулирование криптографии, безопасность цепочек поставок, безопасность новых технологий (ИИ, IoT), нехватка квалифицированных кадров.
- **Сотрудничество:** Существует на уровне международных организаций (ООН, Интерпол, ENISA) для борьбы с киберпреступностью и выработки общих стандартов.

2. Информационная безопасность в РФ.

- **Законодательная база:** Развитая система законов: 152-ФЗ (ПДн), 149-ФЗ (об информации), 98-ФЗ (коммерческая тайна), 256-ФЗ (КИИ), 63-ФЗ (ЭП), 390-ФЗ (о безопасности), законы о

гос. тайне, регулирование интернета (97-ФЗ, ст. 15.3 149-ФЗ), ИИ (331-ФЗ). Ключевые регуляторы: ФСТЭК, ФСБ, Роскомнадзор.

- **Специфика:** Акцент на суверенитет (локализация данных ПДн, "Великий файрвол"), защиту критической инфраструктуры (КИИ), государственный контроль в сфере криптографии (лицензирование ФСБ/ФСТЭК), обязательную сертификацию СЗИ для КИИ.
- **Триада ИБ:** Официально закреплена в 149-ФЗ как конфиденциальность, целостность, доступность информации.
- **Тренды:** Импортозамещение ПО и СЗИ, развитие отечественных ОС (Astra Linux, РЕД ОС), усиление контроля за интернет-коммуникациями и соцсетями.

3. Законодательство в области защиты персональных данных (ПДн) в РФ.

- **Основной закон:** Федеральный закон № 152-ФЗ "О персональных данных".
- **Ключевые положения:**
  - **Определение ПДн:** Любая информация, относящаяся к прямо или косвенно определенному/определяемому физ. лицу (ФИО, паспорт, адрес, тел., email, IP, биометрия и т.д.).
  - **Принципы обработки:** Законность, справедливость, конкретность целей, соответствие объема целям, точность, хранение в идентифицируемой форме не дольше необходимого.
  - **Согласие субъекта:** Общее правило – требуется письменное (в т.ч. электронное) согласие субъекта на обработку его ПДн (исключения - ФЗ, договор, угроза жизни и т.д.).

- **Обязанности оператора:** Обеспечение конфиденциальности и безопасности ПДн (технические и организационные меры), уведомление Роскомнадзора, назначение ответственного за обработку ПДн.
- **Локализация данных:** Базы данных с ПДн граждан РФ должны храниться и обрабатываться на территории РФ (ст. 18 152-ФЗ).
- **Права субъекта ПДн:** На доступ, уточнение, блокирование, уничтожение, отзыв согласия.
- **Ответственность:** Административная (ст. 13.11 КоАП), уголовная (ст. 137 УК РФ), гражданско-правовая.

4. Нормативные требования в области информационной безопасности.

- **Многоуровневая система:**
  1. **Федеральные законы:** Устанавливают основные принципы, требования и ответственность (152-ФЗ, 149-ФЗ, 256-ФЗ, 98-ФЗ, 63-ФЗ, 390-ФЗ и др.).
  2. **Постановления Правительства РФ:** Детализируют требования законов (напр., Постановления к 152-ФЗ о мерах защиты ПДн, к 256-ФЗ о критериях КИИ).
  3. **Приказы и стандарты регуляторов (ФСТЭК, ФСБ):** Конкретные технические и организационные требования:
     - **ФСТЭК:** Приказы о защите ПДн, о требованиях к СЗИ, о порядке аттестации объектов КИИ, стандарты серии ГСТ Р (напр., по СОВ, АВЗ).
     - **ФСБ:** Требования к криптографической защите, СКЗИ, защите от НСД, порядку лицензирования деятельности в области шифрования.

4. **Отраслевые стандарты и требования (ЦБ РФ - СТО БР ИББС, Минздрав и др.).**
5. **Международные и национальные стандарты (ISO 27001, ГОСТ Р ИСО/МЭК 27001).**

5. Угрозы безопасности защищаемой информации.

- **Классификация по источнику:**
  - **Внешние:** APT-группы, хакеры, конкуренты, киберпреступники (DDoS, атаки на цепочку поставок).
  - **Внутренние:** Инсайдеры (обиженные/сочувствующие сотрудники), небрежный персонал.
- **Классификация по способу реализации:**
  - **Вредоносное ПО (Malware):** Вирусы, черви, трояны, шифровальщики (Ransomware), бэкдоры, шпионское/сталкерское ПО, криптоджекинг.
  - **Социальная инженерия:** Фишинг (email), квишинг (QR-коды), вишинг (телефон), смишинг (SMS), претекстинг (вымышленные сценарии), фарминг.
  - **Сетевые атаки:** Несанкционированный доступ (НСД), эксплуатация уязвимостей, перехват трафика (сниффинг), подмена (спуфинг), DDoS, атаки "человек посередине" (MitM).
  - **Атаки на приложения:** Инъекции (SQL, XSS), эксплуатация небезопасных настроек/API.
  - **Физические угрозы:** Кража оборудования, носителей данных, повреждение инфраструктуры, несанкционированный физический доступ.
  - **Угрозы доступности:** Отказы оборудования, стихийные бедствия, ошибки персонала.

- **Утечки информации:** Неправомерный доступ, хищение данных, неконтролируемое распространение.

6. Способы защиты информации. Аппаратные и программные средства обеспечения ИБ.

- **Способы защиты:**
  - **Технические:** Шифрование, контроль доступа, межсетевое экранирование, АВЗ, СОВ/СОП, DLP, резервное копирование, системы аутентификации.
  - **Организационные:** Политики и процедуры ИБ, обучение пользователей, управление инцидентами, аудит, разделение обязанностей, физическая защита.
  - **Правовые:** Соблюдение законодательства, договоры NDA.
- **Аппаратные средства:**
  - Аппаратные межсетевые экраны (NGFW).
  - Аппаратные модули безопасности (HSM) для криптографии.
  - Средства контроля физического доступа (СКУД): считыватели, замки.
  - Средства защиты от утечек по побочным каналам.
  - Защищенные серверы и рабочие станции.
- **Программные средства:**
  - Программные МЭ (брандмауэры), в т.ч. в составе ОС.
  - Антивирусное ПО (АВЗ).
  - Системы обнаружения/предотвращения вторжений (IDS/IPS).
  - Системы предотвращения утечек данных (DLP).
  - Средства криптографической защиты (СКЗИ): шифрование дисков, ЭЦП, VPN.
  - Средства резервного копирования.

- Средства управления доступом (IAM), системы двухфакторной аутентификации (2FA).
- Системы мониторинга безопасности (SIEM).

7. Анализ информационной системы для определения требований к защите информации.

- **Цель:** Выявить активы, угрозы, уязвимости и определить необходимый уровень защищенности и соответствующие меры защиты.
- **Этапы:**
  1. **Идентификация активов:** Какая информация обрабатывается (ПДн, комм. тайна, гос. тайна)? Какие системы, серверы, сети, приложения используются? Кто пользователи?
  2. **Оценка ценности активов:** Какой ущерб возможен при нарушении конфиденциальности, целостности, доступности каждого актива?
  3. **Идентификация угроз:** Какие угрозы актуальны для данных активов и среды функционирования ИС? (См. Вопрос 5).
  4. **Анализ уязвимостей:** Какие слабые места (технические, организационные) есть в ИС, которые могут быть использованы угрозами? Сканирование, аудит настроек, анализ политик.
  5. **Оценка рисков:** Определение вероятности реализации угрозы через найденную уязвимость и величины потенциального ущерба. Ранжирование рисков.
  6. **Определение требований к защите:** На основе оценки рисков, ценности активов и **нормативных требований**

(законы 152-ФЗ, 256-ФЗ, приказы ФСТЭК/ФСБ, отраслевые стандарты) формулируются конкретные требования:

- Класс защищенности ИС (для ПДн по 152-ФЗ, для КИИ по 256-ФЗ).
- Необходимые организационные меры (политики, обучение).
- Необходимые технические меры (типы СЗИ: МЭ, СОВ, DLP, СКЗИ, АВЗ, резервирование и их характеристики).
- Требования к физической защите.
- Требования к персоналу.

7. **Разработка модели угроз и модели нарушителя:** Формализация потенциальных атак.

8. Сетевая безопасность. Управление сетевыми настройками. Межсетевое экранирование в отечественных ОС.

- **Сетевая безопасность:** Комплекс мер по защите сетевой инфраструктуры и данных, передаваемых по сети, от НСД, перехвата, искажения, блокирования. Ключевые принципы: сегментация, контроль доступа, защита периметра, шифрование трафика, мониторинг.
- **Управление сетевыми настройками:**
  - Настройка сетевых интерфейсов (IP, маска, шлюз, DNS).
  - Конфигурация маршрутизации (таблицы маршрутизации).
  - Управление сетевыми службами (включение/отключение ненужных).
  - Настройка VLAN для сегментации сети.
  - Конфигурация безопасных протоколов (SSH вместо Telnet, SNMPv3).

    - Регулярное обновление ПО и прошивок сетевого оборудования.
- **Межсетевое экранирование (МЭ, Firewall):** Техническое средство (аппаратное или программное), фильтрующее сетевой трафик между сетями с разным уровнем доверия (напр., Интернет и внутренняя сеть) на основе заданных правил (адреса, порты, протоколы, состояние соединения). Типы: пакетные, stateful, NGFW (с проверкой содержимого, IDS/IPS, фильтрацией URL).
- **В отечественных ОС (Astra Linux, РЕД ОС):**
    - **Основной инструмент:** `iptables` (устаревает) или `nftables` (современная замена) - встроенные в ядро Linux подсистемы фильтрации трафика. Управляются через одноименные утилиты командной строки или графические оболочки (вроде `gufw` или встроенных в центр управления ОС).
    - **Фронтенды:** ОС часто предоставляют собственные графические интерфейсы или утилиты для упрощенной настройки базовых правил МЭ (разрешить/запретить службы).
    - **Специализированные МЭ:** Возможно использование сертифицированных ФСТЭК программных МЭ (например, "Континент" от Код Безопасности) поверх ОС или в виде отдельных дистрибутивов.
    - **Особенности:** Настройка ведется в соответствии с требованиями руководящих документов ФСТЭК. Важно обеспечить централизованное управление и мониторинг правил.

9. Настройка брандмауэра, работа с VPN туннелями, ключами в отечественных ОС.

- **Настройка брандмауэра (МЭ):** (См. пункт 8). В отечественных ОС:
  - Определение зон доверия (интерфейсы).
  - Формирование правил (цепочки `INPUT`, `OUTPUT`, `FORWARD` для `iptables/nftables`):
    - Разрешение/запрет трафика по протоколам (TCP, UDP, ICMP).
    - Указание портов источника/назначения.
    - Указание адресов источника/назначения.
    - Указание сетевых интерфейсов.
    - Обработка состояний соединений (`ESTABLISHED, RELATED`).
  - Настройка политик по умолчанию (`DROP` или `REJECT` для входящего/пересылаемого трафика).
  - Сохранение правил для автоматической загрузки при старте (`iptables-save`, `nft list ruleset > /etc/nftables.conf`).
- **VPN (Virtual Private Network):** Технология создания защищенного ("зашифрованного туннеля") поверх ненадежной сети (Интернет). Обеспечивает конфиденциальность и целостность передаваемых данных.
- **Работа с VPN туннелями и ключами в отечественных ОС:**
  - **Типы VPN:** Часто используются IPSec (на сетевом уровне) и OpenVPN (на прикладном уровне). Для соответствия требованиям ФСБ/ФСТЭК требуется использование сертифицированных СКЗИ.
  - **Настройка VPN-клиента:**

    - Установка необходимого ПО (`openvpn`, `strongswan`, `libreswan`, или проприетарные клиенты сертифицированных СКЗИ).
    - Импорт конфигурации файла и файлов ключей/сертификатов (предоставленных администратором VPN-сервера).
    - Настройка параметров подключения (адрес сервера, порт, протокол, шифры).
    - Управление соединением (запуск/остановка службы или через GUI).
- **Настройка VPN-сервера:** Более сложная, требует настройки демона (`openvpn`, `strongswan`), генерации инфраструктуры ключей (сертификатов), настройки аутентификации (PSK, сертификаты), управления маршрутизацией.
- **Работа с ключами:**
    - **Типы ключей:** Предварительные общие ключи (PSK - проще, но менее безопасно), Асимметричные ключи (пары открытый/закрытый) на основе сертификатов X.509 (безопаснее, требует PKI).
    - **Генерация:** Используются утилиты (`openssl` для сертификатов, `ipsec pki` для StrongSwan) или инструменты УЦ.
    - **Хранение:** Ключи (особенно закрытые!) должны храниться защищенно (специальные каталоги с ограниченными правами, токены/смарт-карты).
    - **Распространение:** Безопасная передача ключей/сертификатов клиентам (физ. носители, защищенные каналы).

- **Сертифицированные СКЗИ:** В РФ для защиты гостайны или КИИ *обязательно* использование VPN на базе СКЗИ, сертифицированных ФСБ (например, КриптоПро CSP, ViPNet CSP). Они предоставляют собственные средства настройки VPN и управления ключами.

10. Системы обнаружения вторжений (СОВ/IDS - Intrusion Detection System).

- **Назначение:** Мониторинг сети или узлов на предмет подозрительной или вредоносной активности, нарушающей политики безопасности. **Обнаруживает** атаки, но не блокирует их автоматически.
- **Типы:**
  - **Сетевые (NIDS - Network IDS):** Анализируют сетевой трафик (на ключевых точках или в зеркальном порту). Примеры: Snort, Suricata.
  - **Узловые (HIDS - Host IDS):** Мониторят активность на конкретном сервере/рабочей станции (логи, изменения файлов, процессы). Примеры: OSSEC, Wazuh, AIDE.
- **Методы обнаружения:**
  - **Сигнатурный (Misuse Detection):** Сравнение активности с базой известных шаблонов атак (сигнатур). Эффективен против известных угроз. Ложные срабатывания редки, но новые атаки не обнаруживаются.
  - **Аномалийный (Anomaly Detection):** Построение модели "нормального" поведения (профиля). Любые отклонения считаются подозрительными. Может находить неизвестные атаки, но высокий уровень ложных срабатываний.
  - **Гибридный:** Комбинация подходов.

- **Компоненты:** Сенсоры (сбор данных), движок анализа (сравнение с сигнатурами/профилями), консоль управления (настройка, просмотр событий).
- **Выход:** Генерация оповещений (алертов) о потенциальных инцидентах безопасности.
- **Отличие от СОП (IPS - Intrusion Prevention System):** СОП *может* автоматически блокировать подозрительный трафик/активность в реальном времени (сброс соединений, блокировка IP).

11. Настройка системы мониторинга, подключение агентов на различных ОС. Настройка правил.

- **Система мониторинга:** Комплекс ПО для сбора, обработки, визуализации и оповещения о метриках и событиях с ИТ-инфраструктуры (серверы, сети, приложения). Примеры: Zabbix, Nagios, Prometheus+Grafana, ELK Stack (для логов).
- **Настройка системы:**
  1. **Установка сервера/серверов мониторинга.**
  2. **Настройка БД для хранения данных.**
  3. **Определение объектов мониторинга:** Какие хосты, сервисы, метрики нужно отслеживать?
  4. **Настройка методов сбора данных:** SNMP, агенты, WMI, JMX, HTTP-запросы и т.д.
  5. **Настройка правил обнаружения (триггеров):** Определение условий, при которых генерируется событие (напр., CPU > 90% 5 мин, сервис не отвечает, свободное место < 10%).
  6. **Настройка оповещений:** Кому, как и при каких условиях отправлять уведомления (Email, SMS, Telegram, Slack). Эскалация при неисправленных проблемах.

7. **Настройка визуализации:** Создание дашбордов, графиков, карт сети.

- **Подключение агентов:**
  - **Агент:** Легковесная программа, устанавливаемая на мониторируемый хост. Собирает метрики и отправляет их на сервер.
  - **Процесс:**
    - **Linux:** Установка пакета агента (напр., `zabbix-agent`, `node_exporter` для Prometheus) из репозитория. Редактирование конфиг-файла (`/etc/zabbix/zabbix_agentd.conf`): указание IP сервера мониторинга, возможно, настройка активных/пассивных проверок, пользовательских параметров. Запуск и включение службы.
    - **Windows:** Установка MSI-пакета агента. Настройка через GUI или конфиг-файл (аналогично Linux): указание сервера, порта, имени хоста. Запуск службы.
    - **Сетевые устройства:** Настройка SNMP-агента на устройстве (community string, версия SNMP, разрешенные IP сервера мониторинга). На сервере мониторинга добавляется устройство с указанием IP и SNMP-параметров.
- **Настройка правил (триггеров):** На сервере мониторинга создаются правила, которые анализируют полученные от агентов/источников данные. Примеры:
  - `{Template OS Linux:system.cpu.util[,idle].avg(5m)}<20%` (Средняя загрузка CPU за 5 мин > 80%).
  - `{Template OS Linux:vfs.fs.size[/,pfree].last()}<10%` (Свободное место на корневом разделе < 10%).

- `{Template ICMP Ping:icmpping.seq(3,1000,0,,)}>0` (Хост недоступен по ICMP).
- `{Template App Zabbix Server:zabbix[wcache,values].last()}>10M` (Размер кеша значений Zabbix сервера превысил 10МБ).

12. Определение класса защищенности ИС.

- **Класс защищенности (КЗ):** Уровень, характеризующий требования к защите информации в ИС от НСД. Определяется на основе анализа:
  - **Категории обрабатываемой информации:** Особой важности, конфиденциальная (гос. тайна, ПДн, коммерческая тайна, персональные данные с особыми категориями), общедоступная.
  - **Масштаб ИС:** Федеральный, региональный, объектовый.
  - **Уровень однородности:** Однородная (однотипные СВТ), неоднородная.
  - **Режим обработки:** Многопользовательский с разграничением/без разграничения доступа, однопользовательский.
  - **Размещение компонентов:** В пределах/за пределами контролируемой зоны.
- **Нормативная база:**
  - **Для ПДн:** Приказ ФСТЭК России № 21, Приказ ФСБ России № 378 (Устанавливают 4 уровня защищенности (УЗ) ПДн). КЗ зависит от типа ПДн (биометрия, спецкатегории, общедоступные и т.д.), объема (более/менее 100 тыс. субъектов) и типа нарушителя.

    - **Для КИИ (ГИС):** Приказ ФСТЭК России № 31 (Устанавливает 3 категории значимости объектов КИИ и 6 классов защищенности ГИС). Зависит от значимости объекта КИИ и типа угроз.
    - **Для гостайны:** Руководящие документы ФСТЭК (РД), устанавливающие классы АС (Автоматизированные системы) в зависимости от грифа секретности информации.
- **Процесс:** Проводится аттестованной организацией или собственными силами (если есть аттестованные специалисты) путем анализа документов на ИС и обследования. Результат - Акт категорирования/классификации. КЗ определяет **обязательный** набор мер защиты (организационных, технических, физических).

13. Определение состава мероприятий по защите информации в соответствии с уровнем защищенности ИС.

- **Основа:** Определенный класс защищенности (КЗ) или уровень защищенности (УЗ) ИС (см. п.12) *диктует* обязательный минимальный набор защитных мероприятий через соответствующие нормативные акты (Приказ 21/378 для ПДн, Приказ 31 для КИИ, РД для гостайны).
- **Типы мероприятий (по ГОСТам и РД):**
    - **Организационные:**
        - Разработка и утверждение организационно-распорядительных документов по ИБ (Положение, политики, инструкции).
        - Назначение ответственных за ИБ и обработку ПДн.
        - Обучение и инструктаж пользователей.

    - Управление доступом (процедуры выдачи/аннулирования прав).
    - Регламентация процессов обработки информации.
    - Планирование восстановления после инцидентов (DRP).
    - Регулярный контроль (аудит) эффективности мер защиты.
- **Технические:**
    - Идентификация и аутентификация пользователей (включая 2ФА при необходимости по КЗ).
    - Управление доступом (разграничение прав, Мандатное/Дискретное управление доступом - МДВ/ДДВ).
    - Защита машинных носителей информации (шифрование).
    - Регистрация событий безопасности (аудит) и защита журналов.
    - Антивирусная защита (АВЗ).
    - Обнаружение (СОВ) и предотвращение (СОП) вторжений.
    - Защита от НСД при загрузке (целостность ОС).
    - Межсетевое экранирование (МЭ).
    - Контроль целостности ПО и информации.
    - Криптографическая защита информации (СКЗИ) при передаче и хранении (особенно для высоких КЗ).
    - Защита виртуализованных сред.
    - Средства доверенной загрузки.
- **Физические:**
    - Охрана помещений, СКУД.

        - Противопожарная защита, контроль среды.
        - Защита линий связи.
        - Защита от утечек по ПЭМИН (для высоких грифов).
- **Состав:** Конкретный перечень и строгость требований к каждому мероприятию (напр., обязательность МДВ, использование СКЗИ определенного класса, частота смены паролей, глубина хранения журналов аудита) жестко регламентированы для каждого КЗ/УЗ в соответствующих приказах ФСТЭК/ФСБ. Выбор мер защиты *начинается* с определения КЗ.

14. Категории персональных данных в соответствии с классификацией Роскомнадзора (на основе 152-ФЗ).

- **Основа:** Статья 10 152-ФЗ выделяет специальные категории ПДн, требующие особых условий обработки. Роскомнадзор, как регулятор, использует эту классификацию.
- **Категории:**
    1. **Общедоступные ПДн:** Данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта или в соответствии с федеральными законами (напр., данные в справочниках, реестрах - ФИО, должность, тел. организации). *Требуется согласие на включение в общедоступный источник.*
    2. **Биометрические ПДн:** Данные, характеризующие физиологические и биологические особенности человека для установления его личности (отпечатки пальцев, ладони, сетчатка глаза, ДНК, изображение лица (фото/видео) *при использовании для идентификации*, рост, вес, группа крови и т.д.). *Требуется письменное согласие субъекта, кроме случаев, связанных с правосудием, госбезопасностью, ОРД.*

3. **Специальные категории ПДн:** Данные, касающиеся:
    - Расовой, национальной принадлежности.
    - Политических взглядов.
    - Религиозных или философских убеждений.
    - Состояния здоровья.
    - Интимной жизни.
    - Судимости.
    - *Требуется письменное согласие субъекта, кроме исключительных случаев (закон, медицина, ОРД и т.д.).*
4. **Иные ПДн:** Все остальные персональные данные, не попавшие в вышеперечисленные категории (ФИО, паспорт, адрес, тел., email, ИНН, СНИЛС, данные о работе, образовании, доходе (если не спецкатегория), IP-адрес (если идентифицирует) и т.д.). *Требуется согласие субъекта (форма не столь строгая, как для биометрии/ спецкатегорий, но лучше письменное/электронное).*

- **Важно:** Обработка биометрических и специальных категорий ПДн без письменного согласия субъекта возможна *только* в строго оговоренных законом исключительных случаях (ст. 10, 11 152-ФЗ). Категория данных напрямую влияет на требуемый УЗ при их обработке (Приказы 21/378).

15. Электронно-цифровые подписи (ЭЦП / ЭП).

- **Определение (63-ФЗ):** Электронные данные, присоединенные к другим электронным данным (подписываемому документу) или логически с ними связанные, используемые для определения лица, подписывающего информацию.
- **Назначение:** Обеспечивает:

- **Юридическую значимость** электронного документа (аналог собственноручной подписи).
- **Целостность документа:** Любое изменение документа после подписания делает ЭП недействительной.
- **Неотрекаемость (Non-repudiation):** Подписавший не может отказаться от факта подписания.

- **Виды ЭП в РФ (63-ФЗ):**
  1. **Простая ЭП (ПЭП):** Использует коды, пароли или иные средства для подтверждения личности. *Юридическая сила только в случаях, прямо предусмотренных законом или соглашением сторон.* Примеры: СМС-код, логин/пароль в Госуслугах, email-подтверждение.
  2. **Неквалифицированная ЭП (НЭП):** Получена с использованием криптографических средств (СКЗИ). Позволяет определить подписанта и проверить целостность документа. *Юридическая сила при наличии дополнительного соглашения сторон или нормативного акта, признающего ее.*
  3. **Квалифицированная ЭП (КЭП):** Неквалифицированная ЭП, но:
     - Создана с использованием **сертифицированных ФСБ** СКЗИ.
     - Ключ проверки ЭП указан в **квалифицированном сертификате**, выданном **аккредитованным Минцифры Удостоверяющим Центром (УЦ)**.
     - *Имеет максимальную юридическую силу, равную собственноручной подписи, во всех случаях, кроме тех, где закон требует бумажный документ с "живой" подписью.*

- **Принцип работы (на примере асимметричной криптографии):**
    1. Подписант генерирует пару ключей: **закрытый (секретный)** и **открытый**.
    2. Закрытый ключ хранится в тайне (токен, смарт-карта). Открытый ключ публикуется в сертификате УЦ.
    3. При подписании: Создается **хэш** документа (уникальное "дайджест"). Хэш **шифруется** закрытым ключом подписанта -> это и есть ЭП.
    4. При проверке: Получатель вычисляет хэш полученного документа. **Расшифровывает** ЭП открытым ключом подписанта (из сертификата). Сравнивает полученный хэш с расшифрованным. Совпадение = подлинность подписи и целостность документа.
- **Области применения:** Электронный документооборот (ЭДО), сдача отчетности в гос. органы (ФНС, ПФР, Росстат), госуслуги, торги, договоры, внутренние корпоративные документы.

16. Системы антивирусной защиты (АВЗ).

- **Назначение:** Обнаружение, блокирование и удаление вредоносного программного обеспечения (Malware) и других компьютерных угроз.
- **Типы вредоносного ПО:**
    - **Вирусы:** Программы, заражающие другие файлы.
    - **Черви (Worms):** Самораспространяющееся ПО, использующее сетевые уязвимости.
    - **Трояны (Trojans):** Маскируются под легитимное ПО, выполняют скрытые вредоносные действия (кража данных, бэкдоры).

    - **Шифровальщики (Ransomware):** Шифруют данные пользователя с требованием выкупа.
    - **Шпионское ПО (Spyware):** Собирает информацию о пользователе без его ведома.
    - **Рекламное ПО (Adware):** Показывает нежелательную рекламу.
    - **Боты / Ботнеты:** Зараженные компьютеры, управляемые злоумышленником удаленно.
    - **Руткиты (Rootkits):** Скрывают свое присутствие и активность в системе.
    - **Криптоджекинг:** Тайное использование ресурсов устройства для майнинга криптовалюты.
- **Компоненты и технологии АВЗ:**
    - **Сканер по требованию (On-Demand Scanner):** Проверка файлов/системы по запросу пользователя.
    - **Сканер в реальном времени (On-Access Scanner / Realtime Protection):** Постоянно мониторит активность (запуск файлов, открытие документов, сетевой трафик) и блокирует угрозы на лету.
    - **Эвристический анализ:** Обнаружение неизвестных угроз по подозрительному поведению или структуре кода.
    - **Сигнатурный анализ:** Обнаружение известных угроз по уникальным шаблонам (сигнатурам) в коде.
    - **Облачный анализ:** Проверка подозрительных файлов в облаке поставщика АВЗ для скорости и использования больших баз угроз.
    - **Поведенческий анализ (HIPS):** Мониторинг поведения процессов в системе на предмет вредоносных действий (изменение системных файлов, внедрение в процессы).

    - **Проактивная защита:** Блокировка эксплойтов, использование технологий типа ASLR, DEP.
    - **Сетевой экран (Firewall):** Часто интегрируется в комплексные АВЗ-решения для контроля сетевого трафика.
    - **Анти-Фишинг / Анти-Спам:** Защита от веб-мошенничества и нежелательной почты.
    - **Контроль устройств:** Управление доступом USB/CD/DVD.
- **Требования в РФ:** Для защиты КИИ и систем, обрабатывающих ПДн, требуется использование АВЗ, сертифицированных ФСТЭК России. Такие АВЗ проходят испытания на эффективность обнаружения и соответствие требованиям регулятора.

17. Криптография. Методы шифрования.

- **Криптография:** Наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности (невозможности незаметного изменения), аутентификации (проверки подлинности) и неотрекаемости информации.
- **Основные задачи:**
    - **Шифрование/Расшифрование:** Преобразование открытого текста (plaintext) в шифртекст (ciphertext) и обратно.
    - **Хэширование:** Преобразование данных в уникальную фиксированную строку (хеш, дайджест). Необратимо. Для проверки целостности.
    - **Электронная подпись:** См. пункт 15.
    - **Генерация псевдослучайных чисел (ГПСЧ).**
- **Типы криптографии:**
    - **Симметричное шифрование (секретный ключ):**

- **Принцип:** Один и тот же ключ используется и для шифрования, и для расшифрования.
- **Преимущества:** Высокая скорость.
- **Недостатки:** Проблема безопасной передачи ключа сторонам. Масштабируемость.
- **Алгоритмы:** AES (Advanced Encryption Standard - самый распространенный), DES (устарел), 3DES, Blowfish, RC4 (небезопасен), ГОСТ 28147-89 (Кузнечик), ГОСТ Р 34.12-2015 (Магма, К