**1. Понятие компьютерного вируса, виды, вредоносные функции, пути распространения, проявление действия**

Компьютерный вирус — это вредоносная программа, которая способна внедряться в другие программы или файлы, распространяться и выполнять нежелательные действия без ведома пользователя.

 Виды вирусов: файловые, загрузочные, сетевые, макровирусы, скриптовые.

 Вредоносные функции: уничтожение или изменение данных, перегрузка системы, кража информации, создание «лазеек» для других программ.

 Пути распространения: съёмные носители, электронная почта, сетевые соединения, вредоносные сайты.

 Проявление действия: торможение системы, удаление файлов, сбои программ, появление сообщений, самопроизвольная перезагрузка.

**2. Основные понятия безопасности информации: конфиденциальность, целостность, доступность**

Информационная безопасность — это состояние защищённости информации от различных угроз, направленных на её уничтожение, подделку, кражу или блокировку.

Три ключевых свойства, определяющие защищённость информации:

* **Конфиденциальность** Обеспечивает защиту информации от несанкционированного доступа. Цель — чтобы только уполномоченные лица могли читать или использовать данные. Примеры реализации: шифрование, аутентификация, ограничение прав доступа.
* **Целостность** Гарантирует, что данные не были изменены, повреждены или уничтожены без разрешения. Она означает точность и корректность данных, сохранение их в исходном виде. Примеры мер: контрольные суммы, хэш-функции, системы обнаружения изменений.
* **Доступность** Обеспечивает возможность своевременного и надёжного доступа к информации для авторизованных пользователей. Важна, например, для систем управления, банков, здравоохранения. Меры обеспечения: резервное копирование, отказоустойчивые системы, балансировка нагрузки.

Эти три характеристики составляют так называемый **треугольник информационной безопасности (CIA: Confidentiality, Integrity, Availability)**. Нарушение любого из этих свойств считается угрозой информационной безопасности.

**3. Виды мер обеспечения информационной безопасности**

Меры защиты информации можно классифицировать по характеру их воздействия и способу реализации. Они охватывают как юридические, так и технические и поведенческие аспекты.

* **Законодательные меры** Включают в себя законы, подзаконные акты и международные соглашения, регламентирующие защиту информации. Примеры: Федеральный закон "О персональных данных", "О государственной тайне", GDPR. Их задача — установить юридическую ответственность за нарушения и определить стандарты защиты.
* **Морально-этические меры** Основаны на принципах добросовестного поведения при работе с информацией. Включают нормы профессиональной этики, внутренние кодексы поведения сотрудников. Примеры: неразглашение служебной информации, честность при работе с данными.
* **Организационные меры** Представляют собой внутренние правила и процедуры организации, направленные на защиту информации. Примеры: разграничение прав доступа, контроль входа в помещения, обучение сотрудников, создание инструкций и регламентов по работе с данными.
* **Технические меры** Предполагают использование физических и электронных средств для предотвращения угроз. Примеры: замки, видеонаблюдение, системы контроля и управления доступом (СКУД), сейфы, экраны конфиденциальности.
* **Программно-математические меры** Это алгоритмические и программные средства защиты информации. Примеры:
  + антивирусы и системы обнаружения вторжений;
  + криптографические методы: шифрование, цифровая подпись, токены;
  + резервное копирование и восстановление;
  + контроль целостности файлов и логирование событий.

Каждая категория мер решает свою задачу, но только комплексное их применение даёт надёжную защиту. Например, даже самое мощное шифрование не спасёт от утечки, если пользователь добровольно откроет доступ злоумышленнику.

**4. Основные защитные механизмы построения систем защиты информации**

Эффективная система информационной безопасности опирается на совокупность базовых защитных механизмов. Эти механизмы реализуются в программных, технических и организационных решениях и направлены на защиту от различных угроз.

* **Идентификация и аутентификация** Это первые и ключевые этапы защиты.
  + **Идентификация** — процесс установления субъекта (например, пользователь вводит логин или предъявляет карту доступа);
  + **Аутентификация** — проверка, действительно ли субъект тот, за кого себя выдаёт (например, проверка пароля, отпечатка пальца, одноразового кода). Современные методы аутентификации включают однофакторную (например, только пароль), двухфакторную (например, пароль + SMS) и многофакторную (добавляется биометрия или устройство).
* **Разграничение доступа (авторизация)** После идентификации и аутентификации система определяет, какие действия разрешены данному пользователю. Реализуется через **политику доступа**, определяющую:
  + какие ресурсы доступны;
  + какие операции разрешены (чтение, запись, удаление);
  + какие условия должны соблюдаться. Механизмы: списки контроля доступа (ACL), матрицы прав, ролевые модели (RBAC).
* **Контроль целостности** Цель — обнаружить любые изменения информации, произошедшие без разрешения. Методы:
  + контрольные суммы;
  + хэш-функции (например, SHA-256);
  + цифровые подписи. Также используется журналирование изменений и мониторинг целостности файлов (например, в системах IDS — intrusion detection systems).

Эти механизмы часто работают в комплексе, формируя систему защиты с многоуровневой архитектурой (defense in depth).

**5. Криптографические механизмы конфиденциальности, целостности и аутентичности информации. Электронная цифровая подпись**

Криптография — это наука и практика защиты информации путём её преобразования (обычно шифрования), чтобы только авторизованные стороны могли её понять или подтвердить её подлинность.

**Криптографические механизмы решают три фундаментальные задачи:**

* **Конфиденциальность** Достигается с помощью **шифрования**, при котором данные преобразуются в нечитаемый вид. Только обладатель соответствующего ключа может расшифровать сообщение. Существуют:
  + **симметричные алгоритмы** (один ключ): AES, DES;
  + **асимметричные алгоритмы** (два ключа — открытый и закрытый): RSA, ElGamal.
* **Целостность** Обеспечивается с помощью **хэш-функций**, которые создают уникальное фиксированной длины значение (хэш) от данных. Если данные изменены — хэш изменится. Примеры: SHA-256, SHA-3. Для дополнительной защиты может использоваться **MAC** (message authentication code) или **HMAC** — хэш с секретным ключом.
* **Аутентичность** Подтверждается через криптографические протоколы, позволяющие убедиться в том, что данные отправлены определённым источником. Часто реализуется с помощью **цифровой подписи**, где открытый ключ позволяет проверить, что данные подписаны соответствующим закрытым ключом.

**Электронная цифровая подпись (ЭЦП)** — это один из важнейших инструментов обеспечения **аутентичности и целостности**. Она представляет собой результат криптографического преобразования, создаваемый с помощью закрытого ключа и привязанный к конкретным данным.

**Свойства ЭЦП:**

* Невозможность подделки: без знания закрытого ключа нельзя создать допустимую подпись;
* Проверяемость: любой может проверить подпись, используя открытый ключ;
* Защита от изменения данных: при изменении хотя бы одного бита данных подпись становится недействительной;
* Юридическая значимость: в ряде стран ЭЦП приравнивается к собственноручной подписи.

ЭЦП применяется в документообороте, онлайн-банкинге, электронных торгах и любых системах, где требуется юридическая обоснованность и подлинность данных.

**6. Классификация антивирусных программ. Программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры. Профилактика заражения вирусом**

Антивирусные программы — это специализированное программное обеспечение, предназначенное для обнаружения, блокировки и удаления вредоносного кода (вирусов, троянов, червей, шпионского ПО и др.).

**Антивирусы классифицируются по принципу действия на несколько типов:**

**1. Программы-детекторы (сканеры)** Основываются на **поиске сигнатур** — уникальных последовательностей байтов, характерных для известных вирусов.

* Работают по принципу: "если найдено совпадение — это вирус";
* Эффективны против известных вирусов;
* Недостаток: не выявляют новые и модифицированные угрозы (неизвестные сигнатуры).

Пример: простые версии антивирусов, основанные только на базе сигнатур.

**2. Программы-доктора (фаги)** Не только обнаруживают вирус, но и **восстанавливают заражённые файлы** — «лечат» их.

* Удаляют вирусный код, восстанавливая оригинальное содержимое;
* Часто сочетаются с детекторами и антивирусными базами;
* Эффективны при распространённых вирусах, где известна структура заражения.

**3. Программы-ревизоры** Работают по принципу **сравнения текущего состояния системы с эталонным**.

* Сохраняют контрольные суммы, размеры и другие характеристики файлов и системных объектов;
* При повторной проверке выявляют подозрительные изменения;
* Позволяют обнаруживать даже неизвестные вирусы, но не всегда точно определяют их характер.

Используются в корпоративной защите и системах аудита целостности.

**4. Программы-фильтры (мониторы)** **Следят за поведением программ в реальном времени** и блокируют подозрительные действия.

* Могут обнаруживать вирусы по действиям, даже если сигнатура неизвестна;
* Защищают системные области, реестр, сетевые соединения, загрузочные секторы;
* Эффективны против современных угроз, включая шифровальщиков и эксплойтов.

Пример: постоянный антивирусный монитор или защитник в ОС.

**Профилактика заражения вирусом**

Надёжная защита требует не только установки антивируса, но и соблюдения общих правил безопасности:

1. **Регулярное обновление антивирусного ПО** — для актуализации сигнатур и правил поведения;
2. **Не открывать подозрительные вложения в письмах** — особенно с расширениями .exe, .scr, .js;
3. **Использование только доверенных источников ПО** — избегать пиратских программ и неофициальных репозиториев;
4. **Ограничение прав пользователя** — не работать под учётной записью администратора без необходимости;
5. **Резервное копирование данных** — особенно критично при угрозе шифровальщиков;
6. **Использование межсетевого экрана (фаервола)** — ограничивает несанкционированный сетевой доступ;

**Обновление операционной системы и программ** — устранение уязвимостей, которыми могут воспользоваться вирусы.