**Лекция 4: Защита от компьютерных вирусов и заражение компьютера**

Какие являются компьютерные вирусы и механизмы их распространения.

Признаки заражения компьютера и методы обнаружения вредоносных программ.

Средства и стратегии защиты от вирусов.

**Компьютерные вирусы и их механизмы распространения:**

Компьютерные вирусы - это вредоносные программы, которые могут внедряться в компьютерную систему и выполнять различные деструктивные действия. Они распространяются различными способами, включая:

**Загрузка из интернета**: Вирусы могут распространяться через вредоносные веб-сайты или загрузки с ненадежных источников.

**Электронная почта**: Вредоносные вложения или ссылки в электронных письмах могут быть использованы для заражения компьютеров.

**Съемные носители**: Зараженные USB-флешки, внешние жесткие диски и другие съемные носители могут передавать вирусы с одного компьютера на другой.

**Уязвимости и эксплоиты**: Злоумышленники могут использовать уязвимости в операционной системе или приложениях для внедрения вирусов.

**Сетевые атаки**: Вирусы могут распространяться через сетевые атаки, такие как черви, которые могут сканировать и инфицировать другие устройства в сети.

**Признаки заражения компьютера и методы обнаружения вредоносных программ:**

Признаки заражения компьютера могут варьироваться в зависимости от типа вредоносной программы, но обычно включают в себя следующие:

**Ухудшение производительности**: Вирусы могут замедлять работу компьютера.

**Неожиданные ошибки и сбои**: Появление ошибок и сбоев в работе системы может свидетельствовать о заражении.

**Измененные файлы и настройки**: Вирусы могут изменять файлы, настройки и реестр системы.

**Спам и всплывающие окна**: Вредоносные программы могут вызывать появление спама и всплывающих окон.

**Антивирусные программы и обнаружение**: Регулярная проверка антивирусным программным обеспечением может обнаруживать вредоносные программы и предупреждать пользователя о возможном заражении.

**Мониторинг сетевой активности**: Мониторинг сетевой активности может выявлять подозрительные попытки связи с внешними серверами.

**Средства и стратегии защиты от вирусов:**

**Антивирусное программное обеспечение**: Установка и регулярное обновление антивирусного программного обеспечения помогает обнаруживать и удалять вирусы.

**Обновления системы и приложений**: Регулярное обновление операционной системы и прикладного программного обеспечения может закрывать уязвимости, которые могут использоваться злоумышленниками.

**Бережное обращение с электронной почтой и вложениями**: Остерегайтесь ненадежных электронных писем и не открывайте вложения от незнакомых отправителей.

**Осторожность при скачивании из интернета**: Скачивайте файлы только с доверенных источников.

**Фильтрация сетевого трафика**: Используйте брандмауэры и средства фильтрации сетевого трафика для блокирования нежелательной активности.

**Обучение и информирование пользователей**: Обучайте пользователей о мерах безопасности, чтобы они могли избегать потенциальных угроз.

**Регулярное резервное копирование данных**: Регулярное создание резервных копий данных помогает восстановить информацию в случае атаки.

**Мониторинг и реагирование на инциденты**: Настраивайте системы мониторинга безопасности и разрабатывайте планы реагирования на инциденты для быстрого обнаружения и устранения угроз.

Защита от вирусов требует комплексного подхода и внимательности со стороны пользователей и администраторов систем.

Код для создания простой утилиты для сканирования файлов и обнаружения вредоносных программ на Python может выглядеть следующим образом.

В данном примере мы будем использовать библиотеку **clamav** для сканирования файлов на вирусы. Убедитесь, что вы установили библиотеку **pyclamav** перед выполнением кода.





 # Замените на путь к файлу, который вы хотите проверить

 Описание команд и синтаксиса:

import pyclamav - Импортируем библиотеку pyclamav, которая предоставляет функции для сканирования файлов на вирусы с использованием ClamAV.

def scan\_file(file\_path): - Определяем функцию scan\_file, которая будет принимать путь к файлу в качестве аргумента.

try...except - Мы используем блок try...except, чтобы обработать возможные ошибки, например, если файл не найден.

with open(file\_path, 'rb') as file: - Мы открываем файл для чтения бинарных данных.

file\_data = file.read() - Считываем содержимое файла в переменную file\_data.

scan\_result = pyclamav.scanfile(file\_data) - Мы сканируем содержимое файла на вирусы и сохраняем результат сканирования в scan\_result.

if...elif...else - Мы анализируем результат сканирования и выводим соответствующее сообщение в зависимости от результата.

if \_\_name\_\_ == "\_\_main\_\_": - Эта конструкция позволяет запускать код только в том случае, если скрипт выполняется как главный (а не импортированный в другой скрипт).

file\_path = "путь\_к\_файлу\_для\_сканирования" - Замените это значение на путь к файлу, который вы хотите проверить на вирусы.

scan\_file(file\_path) - Мы вызываем функцию scan\_file с указанным путем к файлу.

Этот код позволит вам сканировать файлы на вирусы с использованием библиотеки ClamAV и получать информацию о результатах сканирования.