A person in a dark suit and white shirt is holding a black spray bottle with a yellow and black radiation symbol on it. They are spraying the bottle towards a computer monitor. The background is a textured, mottled green and brown. A computer keyboard is visible in the foreground.

# Вирусы и антивирусные программы

# Что такое вирус?!

**Вирус** - программа, способная присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера.

# Этапы развития

## ВИРУСОВ

- **Доисторический.** Вирусы-легенды и документально подтверждённые инциденты на «мейнфреймах» 1970-80-х годов.
- **«Доинтернетовский».** В основном ему присущи «классические вирусы» для MS-DOS.
- **Интернет-этап.** Многочисленные черви, эпидемии, приводящие к колоссальным убыткам.
- **Современный, криминальный этап.** Использование интернета в преступных целях.

# Признаки проявления вирусов

- прекращение работы или неправильная работа ранее успешно функционировавших программ
- медленная работа компьютера
- невозможность загрузки операционной системы
- исчезновение файлов и каталогов или искажение их содержимого
- изменение даты и времени модификации файлов
- изменение размеров файлов
- неожиданное значительное увеличение количества файлов на диске
- существенное уменьшение размера свободной оперативной памяти
- вывод на экран непредусмотренных сообщений или изображений
- подача непредусмотренных звуковых сигналов
- частые зависания и сбои в работе компьютера

# Каналы распространения

1. Накопители
2. Электронная почта
3. Системы обмена мгновенными сообщениями
4. Веб-страницы
5. Интернет и локальные сети

# Типология вирусов

- Стандартные COM-EXE-TSR – вирусы
- "Стелс"-вирусы
- Полиморфные вирусы
- Макровирусы
- Трояны
- Перезаписывающие вирусы
- Вирусы-компаньоны
- Вирусы-звенья
- Файловые черви
- Паразитические вирусы



# Стандартные COM-EXE-TSR-

## вирусы

Проникают в различные выполняемые файлы, сектора дисков и в оперативную память, вирусы обживают новую среду обитания: плодятся и размножаются. Создаются новые копии вируса и поражаются новые объекты. Обычно эти вирусы довольно примитивны. Обнаружить их можно практически сразу по некорректной работе компьютерной системы, уменьшению количества доступных системных ресурсов (например, дисковой и оперативной памяти) либо по изменению длины выполняемых файлов.



# "Стелс"-вирусы


Представители этого класса используют различные средства для маскировки своего присутствия в системе. Обычно это достигается путём перехвата ряда системных функций, ответственных за работу с файлами. "Стелс"-технологии делают невозможным обнаружение вируса без специального инструментария. Вирус маскирует и приращение длины поражённого объекта (файла), и своё тело в нём, "подставляя" вместо себя "здоровую" часть файла.



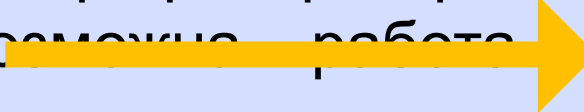


# Полиморфные вирусы

Эти вирусы используют специальные механизмы, которые затрудняют их обнаружение. Обычно такие вирусы содержат код генерации шифровщика и расшифровщика собственного тела. Создаваемые генератором шифровщики (и соответствующие расшифровщики) обычно изменяются во времени. В полиморфных вирусах расшифровщик не является постоянным - для каждого инфицированного файла он свой. По этой причине зачастую нельзя установить инфицированный файл по характерной для данного вируса строке (сигнатуре). Вследствие этого некоторые антивирусные средства в принципе не ловят полиморфные вирусы (наглядный пример такого рода - весьма популярный антивирус Avast).



# Макровирусы

Они используют возможности макроязыков, встроенных в различные системы обработки информации (текстовые редакторы, электронные таблицы и т.п.). Сегодня подобные вирусы широко распространены в системах MS Word и Excel. В этих пакетах вирусы захватывают управление при открытии или закрытии заражённого файла, перехватывают некоторые файловые функции и затем заражают файлы, к которым происходит обращение. В какой-то степени подобные вирусы можно назвать "резидентными", так как они активны только в своей среде - соответствующем приложении. Особенностью таких вирусов является то, что они способны "жить" не только на отдельных компьютерах, а быстро распространяться по сети на все машины, где ~~всёмогуще работа~~  соответствующих приложений.

# Трояны

Трояны способны, например, перехватывать введенные пользователем пароли и записывать их в файл или пересылать автору. В этом и заключается основное, на мой взгляд, отличие троянов от вирусов: вирусы самодостаточны, а трояны должны "связываться" со своим автором. То есть если бороться с вирусами можно только одним способом - вылавливать и уничтожать, - то для защиты от троянов можно перекрыть им возможность связи с автором.



# Перезаписывающие вирусы

Вирусы данного типа записывают своё тело вместо кода программы, не изменяя названия исполняемого файла, вследствие чего исходная программа перестаёт запускаться. При запуске программы выполняется код вируса, а не сама программа.



# Вирусы-компаньоны

Создают свою копию на месте заражаемой программы, но в отличие от перезаписываемых не уничтожают оригинальный файл, а переименовывают или перемещают его.



# Вирусы-компаньоны

Создают свою копию на месте заражаемой программы, но в отличие от перезаписываемых не уничтожают оригинальный файл, а переименовывают или перемещают его.



# Вирусы-звенья

Не изменяют код программы, а заставляют операционную систему выполнить собственный код, изменяя адрес местоположения на диске заражённой программы на собственный адрес. После выполнения кода вируса управление обычно передаётся вызываемой пользователем программе.



# Файловые черви

Файловые черви создают собственные копии с привлекательными для пользователя названиями (например, Game.exe, install.exe и др.) в надежде на то, что пользователь их запустит.





# Паразитические вирусы

Файловые вирусы, изменяющие содержимое файла, добавляя в него свой код. При этом заражённая программа сохраняет полную или частичную работоспособность. Код может внедряться в начало, середину или конец программы. Код вируса выполняется перед, после или вместе с программой, в зависимости от места внедрения вируса в программу.

# Методики обнаружения и защиты от вирусов

Сканирование

Эвристический анализ

Обнаружение изменений

Резидентные мониторы

Вакцинирование программ

Аппаратная защита от вирусов

# Сканирование

Антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Под сигнатурой понимается уникальная последовательность байт, принадлежащая вирусу, и не встречающаяся в других программах.



# Эвристический анализ

Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаются обнаружить в них код, характерный для вирусов.



# Обнаружение изменений

Антивирусные программы могут предварительно запомнить характеристики всех областей диска, которые подвергаются нападению вируса, а затем периодически проверять их (отсюда происходит их название программы-ревизоры). Если будет обнаружено изменение, тогда возможно что на компьютер напал вирус.



# Резидентные мониторы

Резидентный монитор сообщит пользователю, если какая-либо программа попытается изменить загрузочный сектор жесткого диска или дискеты, выполнимый файл.



# Вакцинирование программ

Для того, чтобы человек смог избежать некоторых заболеваний, ему делают прививку. Существует способ защиты программ от вирусов, при котором к защищаемой программе присоединяется специальный модуль контроля, следящий за ее целостностью. При этом может проверяться контрольная сумма программы или какие-либо другие характеристики. Когда вирус заражает вакцинированный файл, модуль контроля обнаруживает изменение контрольной суммы файла и сообщает об этом пользователю.



# Аппаратная защита от вирусов

На сегодняшний день одним из самых надежных способов защиты компьютеров от нападений вирусов являются аппаратно-программные средства.

Обычно они представляют собой специальный контроллер, вставляемый в один из разъемов расширения компьютера и программное обеспечение, управляющее работой этого контроллера



# Киберпреступность

Поскольку компьютерному хакерству уже больше 30 лет, у правительств было достаточно времени, чтобы разработать и принять ряд законов по борьбе с киберпреступностью. В настоящее время почти во всех развитых странах в той или иной форме имеется набор законодательных актов, посвященных противостоянию хакерству и электронным кражам информации, которое можно использовать для наказания киберпреступников. Часто предпринимаются попытки сделать подобные законы еще более строгими,

# Наказания за киберпреступления



**Кэвин Митник** самый знаменитый «черный» хакер, был пойман компьютерным экспертом Цутому Симамура. Митника приговорили к 46 месяцам реального и трем годам условного заключения. Вдобавок его обязали выплатить

Владимир Левин, русский компьютерный эксперт, взломавший сеть Citibank и укравший 10 млн USD. Его арестовал Интерпол в Великобритании в 1995 году. Суд приговорил Владимира к 3 годам лишения свободы и штрафу в 240015 USD



**Матеас Калин, румынский хакер, был арестован вместе с пятью гражданами США по обвинению в краже более 10 млн USD у компании Ingram Micro из Санта-Аны, Калифорния. В настоящее время (конец 2004 года) Матеас и его сообщники ожидают решения суда, которое грозит обернуться 90 годами тюремного**



# Вместо заключения

При всей серьезности проблемы ни один вирус не способен принести столько вреда, сколько побелевший пользователь с дрожащими руками!!!