«Вирусы и антивирусные программы".

Персональный компьютер играет в жизни современного человека важную роль, поскольку он помогает ему почти во всех областях его деятельности. Современное общество все больше вовлекается в виртуальный мир Интернета. Но с активным развитием глобальных сетей актуальным является вопрос информационной безопасности, так как проникающие их сети вирусы могут нарушить целостность и сохранность вашей информации.

Защита компьютера от вирусов – это та задача, решать которую приходится всем пользователям, и особенно тем, кто активно пользуется Интернетом или работает в локальной сети.

Компьютерный вирус

https://youtu.be/zKPGQdeyxvY

Кто и зачем создает компьютерные вирусы. Какие бывают компьютерные вирусы

https://youtu.be/-k786KxeSzE

Компьютерные вирусы и антивирусные программы.

https://youtu.be/Tnz2ZqtNdOA

История возникновения вирусов

Компьютерные вирусы, как таковые, впервые появились в 1986 году, хотя исторически возникновение вирусов тесно связано с идеей создания самовоспроизводящихся программ. Одним из "пионеров" среди компьютерных вирусов считается вирус "Brain", созданный пакистанским программистом по фамилии Алви. Только в США этот вирус поразил свыше 18 тыс. компьютеров. В начале эпохи компьютерных вирусов разработка вирусоподобных программ носила чисто исследовательский характер, постепенно превращаясь на откровенно вражеское отношение к пользователям безответственных, и даже криминальных "элементов".

Признаки заражения компьютера:

- некоторые программы перестают работать или работают с ошибками;
- размер некоторых исполняемых файлов и время их создания изменяются. В первую очередь это происходит с командным процессором, его размер увеличивается на величину размера вируса;
- на экран выводятся посторонние символы и сообщения, появляются странные видео и звуковые эффекты;
- работа компьютера замедляется и уменьшается размер свободной оперативной памяти;
- некоторые файлы и диски оказываются испорченными (иногда необратимо, если вирус отформатирует диск);
- компьютер перестает загружаться с жесткого диска.

Типы вредоносных программ:

- **Вирусы, черви, троянские и хакерские программы**. Эта группа объединяет наиболее распространенные и опасные категории вредоносных программ.
- **Шпионское, рекламное ПО**, программы скрытого дозвона. Это потенциально опасное ПО, которое может причинить неудобство пользователю и ли нанести значительный ущерб.
- **Потенциально опасное ПО**. Эта группа включает программы, которые не являются вредоносными или опасными, однако при некотором стечении обстоятельств могут быть использованы для нанесения вреда вашему ПК.

Содержание

Что такое вирусы?

Компьютерным вирусом – называется вредоносная программа, обладающая способностью самовоспроизведению (размножению), способная внедрять свои копии в файлы, загрузочные секторы дисков и документы , засорению компьютера и выполнению других нежелательных действий.

Общее между биологическим вирусом и компьютерным:

1. Способность к размножению.
2. Вред для здоровья человека и нежелательные действия для компьютера.
3. Скрытность, т.к. вирусы имеют инкубационный период.

Классификация вирусов

по среде обитания

по способу заражения среды обитания

по степени воздействия

по свойствам алгоритма

По среде обитания вирусы подразделяются на:

- ***Сетевые вирусы*** распространяются по различным компьютерным сетям.
- ***Файловые вирусы*** внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE.
- ***Загрузочные вирусы*** внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord**).**
- ***Файлово-загрузочные вирусы*** заражают как файлы, так и загрузочные сектора дисков.
- ***Макровирусы*** заражают документы, выполненные в некоторых прикладных программах (например, Word).

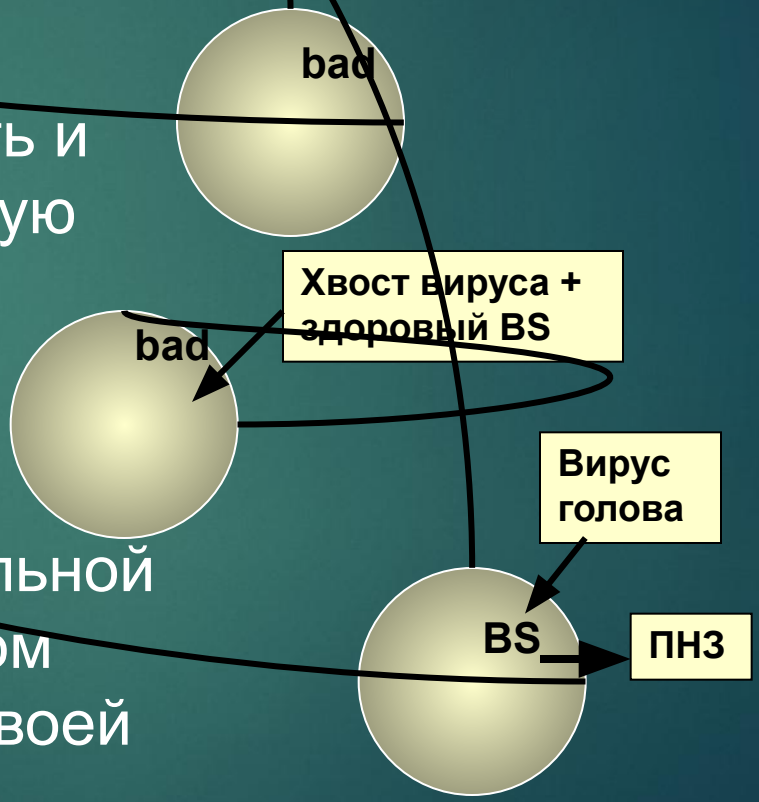
Загрузочный вирус

Нормальная схема начальной загрузки следующая: ПНЗ (ПЗУ) ПНЗ(диск) система.

ПНЗ – программа начальной загрузки.

Действия вируса:

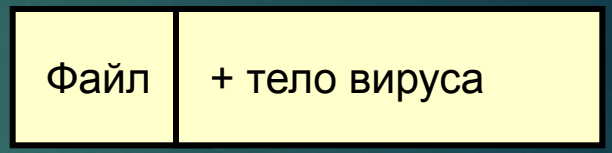
- Выделяет на диске область и помечает ее как недоступную для ОС.
- Копирует в выделенную область диска свой хвост.

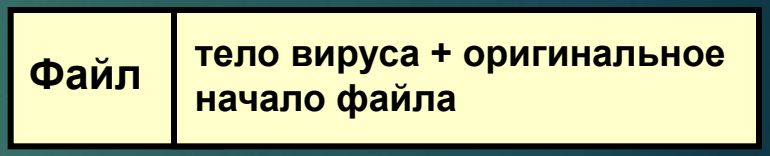


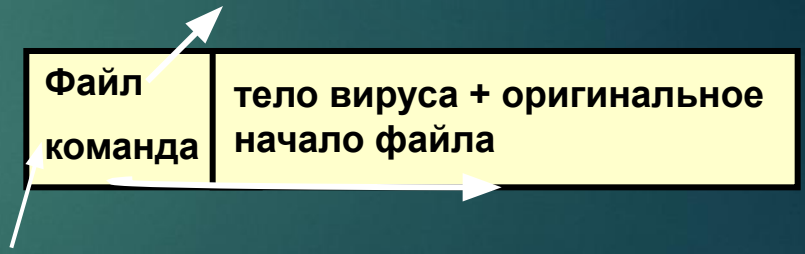
3. Замещает программу начальной загрузки (ПНЗ) в загрузочном секторе (BS, настоящем) своей головой.
4. Организует цепочку передачи управления по схеме: ПНЗ (ПЗУ) Вирус ПНЗ(диск) система

Файловый вирус

1. Дописывает к файлу собственную копию (тело вируса);
2. Сохраняет в этой копии оригинальное начало файла;
3. Замещает оригинальное начало файла на команду передачи управления на тело вируса







По способу заражения среды обитания вирусы подразделяются на:

- *резидентные:*

  при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

- *нерезидентные:*

  не заражают память компьютера и являются активными ограниченное время

По степени воздействия вирусы подразделяются на:

- **неопасные**, *не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах*

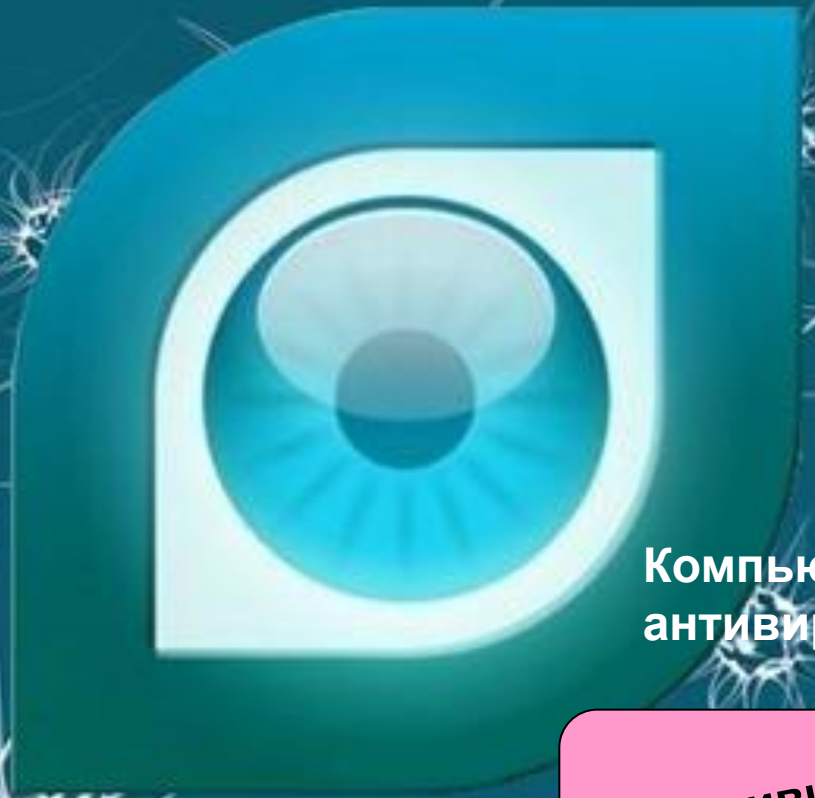
- **опасные вирусы**, *которые могут привести к различным нарушениям в работе компьютера*

- **очень опасные**, *воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.*

По особенностям алгоритма:

- **Простейшие вирусы - паразитические**, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.
- **Вирусы-репликаторы**, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.
- **Вирусы-невидимки**, называемые **стелс-вирусами**, очень трудно обнаружить и обезвредить - они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.
- **Вирусы-мутанты –** вирусы, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов, их наиболее трудно обнаружить.
- **Квазивирусные или «троянские» программы**, которые не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Виды Антивирусов



Антивирусы-
-фильтры

Антивирусы-
-детекторы

Компьютерные вирусы и антивирусные программы.

Антивирусы-
- доктора

Антивирусы-
-вакцинаторы

Антивирусной называется программа выполняющая одну или несколько из следующих функций: защиту данных от разрушения, обнаружение вируса, нейтрализация вируса.

Антивирусы-фильтры

Антивирусы-фильтры или сторожа - **п**рограммы, которые уведомляют пользователя обо всех действиях на его компьютере. Если вирус попытается проникнуть на ваш ПК или, наоборот, украсть пароль и отправить его злоумышленнику, сторож спросит: «Разрешить или запретить выполнение операции?». К сожалению, работа с данным типом защиты требует определённых навыков, ведь далеко не каждый знает, что обозначает тот или иной процесс.

Антивирусы-детекторы

Они контролируют уязвимые и поэтому наиболее атакуемые компоненты компьютера, запоминают состояние служебных областей и файлов, а в случае обнаружения изменений сообщают пользователю. Их нужно регулярно обновлять, ведь вредоносные программы быстро мутируют и размножаются. Какой антивирус-детектор лучше – не знает никто, хотя в интернете можно найти многочисленные тесты и сравнительные обзоры антивирусов. И дело не в стоимости, стране-производителе или размере баз для обновления. Главное почаще обновлять его и не забывать продлевать лицензию.

Антивирусы-вакцинаторы

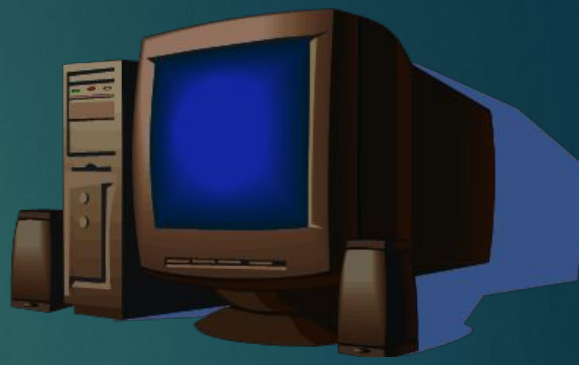
Вакцины– имитируют заражение файлов вирусами. Вирус будет воспринимать их зараженными и не будет внедряться.

Уже заражённые компьютеры сложно вылечить с помощью детектора или фильтра. В очень тяжёлых случаях на помощь приходят программы-вакцинаторы. Даже дорогой лицензионный антивирус не всегда может справиться с червём или троянской программой. К числу наиболее популярных вакцинаторов относятся Anti Trojan Elite, Trojan Remover или Dr.Web CureIt!. Последний, кстати, лечит практически любую инфицированную систему, но для регулярной защиты ПК его недостаточно.

Антивирусы-доктора

Доктора – предназначены для обнаружения и устранения известных им вирусов, удаляя их из тела программы и возвращая ее в исходное состояние. Наиболее известными представителями являются Dr.Web, AidsTest, Norton Anti Virus.

Пути проникновения вирусов на компьютер:



- Глобальная сеть Internet
- Электронная почта
- Локальная сеть
- Компьютеры «Общего назначения»
- Пиратское программное обеспечение
- Ремонтные службы
- Съемные накопители, на которых находятся заражённые вирусом файлы
- Жёсткий диск, на который попал вирус
- Вирус, оставшийся в оперативной памяти после предшествующего пользователя

Методы защиты от компьютерных вирусов

- Установите на свой персональный компьютер современную антивирусную программу.
- Перед просмотром информации принесенной на флэш-карте (дискете) с другого компьютера проверьте носитель антивирусом.
- После разархивирования архивных файлов сразу проверьте их на вирусы (не все антивирусные программы могут искать вредоносный код в архивах или могут делать это не корректно).

Методы защиты от компьютерных вирусов

- Периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом – запускайте раз в неделю, а то и чаще).
- Как можно чаще делайте резервные копии важной информации (backup).
- Используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет.
- Настройте браузер (программа просмотра Интернет страниц – IE, Opera и т.д.) для запрета запуска активного содержимого html- страниц.

Примеры антивирусных программ:

Антивирус Касперского

ESET NOD32

Dr. Web

Антивирус Касперского

Антивирус Касперского — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS.

Антивирус NOD32

Проактивная защита и точное обнаружение угроз. Антивирус ESET NOD32 разработан на основе передовой технологии ThreatSense®. Ядро программы обеспечивает проактивное обнаружение всех типов угроз и лечение зараженных файлов (в том числе, в архивах) благодаря широкому применению интеллектуальных технологий, сочетанию эвристических методов и традиционного сигнатурного детектирования.

Dr.Web

Dr.Web — это семейство антивирусов, предназначенных для защиты от почтовых и сетевых червей, руткитов, файловых вирусов, троянских программ, стелс-вирусов, полиморфных вирусов, бестелесных вирусов, макровирусов, вирусов, поражающих документы MS Office, скрипт-вирусов, шпионского ПО (spyware), программ-похитителей паролей, клавиатурных шпионов, программ платного дозвона, рекламного ПО (adware), потенциально опасного ПО, хакерских утилит, программ-люков, программ-шуток, вредоносных скриптов и других вредоносных объектов, а также от спама, скаминг-, фарминг-, фишинг-сообщений и технического спама.

THE END

Виды вирусов:

Троянский конь (Trojans)

Шпион (Spyware)

Зомби (Zombie)

Фишинг (Phishing)

Червь (Worm)

Фарминг

Рутkиты

Троян или троянский конь (Trojans)

Троян или троянский конь (Trojans) - это программа, которая находится внутри другой, как правило, абсолютно безобидной программы, при запуске которой в систему инсталлируются программа, написанная с целью нанести ущерб целевому компьютеру путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

Зомби (Zombie)

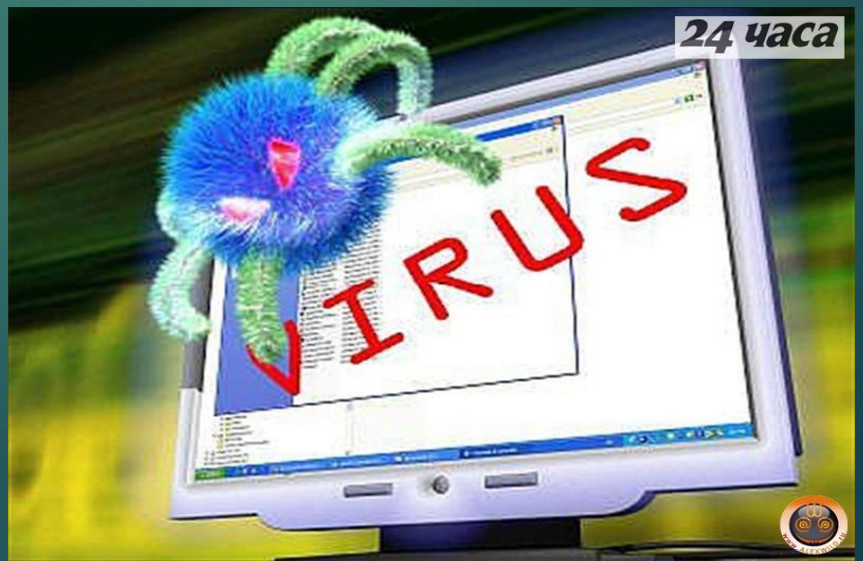
Зомби (Zombie) - это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые рассылается огромное количество нежелательных сообщений электронной почты, а также распространяются вирусы и другие вредоносные программы.

Червь (Worm)

Червь (Worm) - это программа, которая тиражируется на жестком диске, в памяти компьютера и распространяется по сети. Особенностью червей является то, что они не несут в себе никакой вредоносной нагрузки, кроме саморазмножения, целью которого является замусоривание памяти, и как следствие, затормаживание работы операционной системы.

Руткиты

Руткиты – программы, установленные и работающие на компьютере без ведома пользователя и прячущие используемые злоумышленниками инструменты от антивирусного ПО. Они представляют значительный риск безопасности для домашних и корпоративных машин и сетей, так как их очень сложно обнаружить. Сами руткиты обычно устанавливаются с помощью вирусов или других вредоносных объектов, поэтому настоятельно рекомендуется постоянно обновлять антивирусную защиту и защиту от шпионов.



Шпионская программа (Spyware)

Шпионская программа (Spyware) - это программный продукт, установленный или проникший на компьютер без согласия его владельца, с целью получения практически полного доступа к компьютеру, сбора и отслеживания личной или конфиденциальной информации. Эти программы, как правило, проникают на компьютер при помощи сетевых червей, троянских программ или под видом рекламы (adware).

Фишинг (Phishing)

Фишинг (Phishing) - это почтовая рассылка имеющая своей целью получение конфиденциальной финансовой информации. Такое письмо, как правило, содержит ссылку на сайт, являющейся точной копией Интернет-банка или другого финансового учреждения. Пользователь, обычно, не догадывается, что находится на фальшивом сайте и спокойно выдает злоумышленникам информацию о своих счетах, кредитных карточках, паролях и т. д.

Фарминг

Фарминг – замаскированная форма фишинга, заключающаяся в том, что при попытке зайти на официальный сайт интернет банка или коммерческой организации, пользователь автоматически перенаправляется на ложный сайт, который очень трудно отличить от официального сайта. Фарминг отличается от фишинга тем, что вместо электронной почты мошенники используют более изощренные методы направления пользователя на фальшивый сайт.