Компьютерная презентация по теме «Компьютерные вирусы»

Содержание

Содержание

Окончание просмотра

Понятие компьютерного вируса

Компьютерный вирус - это специально написанная небольшая программа, которая может приписывать себя к другим программам (т.е. заражать их), а также выполнять различные вредные действия на компьютере.

Название «вирус» по отношению к компьютерным программам пришло из биологии именно по признаку способности к саморазмножению.

Компьютерные вирусы имеют много сходного с живыми микроорганизмами, это:

- *скрытность;*
- *способность к размножению;*
- *приспособляемость к среде;*
- *передвижение;*
- *самопроизвольное внедрение в другие объекты и т.д.*

Содержание

Далее

Понятие компьютерного вируса

В результате заражения происходят следующие феномены, которые являются признаками заражения компьютера:

• некоторые программы перестают работать или работают с ошибками;
• размер некоторых исполнимых 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.

Содержание Назад Далее

Понятие компьютерного вируса

По величине вредных воздействий вирусы можно разделить на 3 группы.

НЕОПАСНЫЕ

- Влияние ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и другими внешними эффектами

ОПАСНЫЕ

- Приводят к сбоям и зависаниям при работе компьютера

ОЧЕНЬ ОПАСНЫЕ

- Приводят к потере программ и данных, форматированию винчестера

Содержание

Назад

История возникновения вирусов

Мнений по поводу рождения первого компьютерного вируса очень много. Известно только одно: на машине Ч. Бэббиджа, считающегося изобретателем первого компьютера, вирусов не было, а на Univax 1108 и IBM 360/370 в середине 1970-х годов они уже были.

Отправной точкой возникновения вирусов можно считать труды Джона фон Неймана по изучению самовоспроизводящихся математических автоматов, которые стали известны в 1940-х годах.

В 1962 г. инженеры из американской компании Bell Telephone Laboratories - В.А. Высотский, Г.Д. Макилрой и Роберт Моррис - создали игру "Дарвин". Игра предполагала присутствие в памяти вычислительной машины так называемого супервизора, определявшего правила и порядок борьбы между собой программ-соперников, создававшихся игроками. Программы имели функции исследования пространства, размножения и уничтожения. Смысл игры заключался в удалении всех копий программы противника и захвате поля битвы.

Содержание

Далее

История возникновения вирусов

Первая «массовая» эпидемия компьютерного вируса произошла в 1986 году, когда вирус Brain «заражал» дискеты массовых персональных компьютеров.

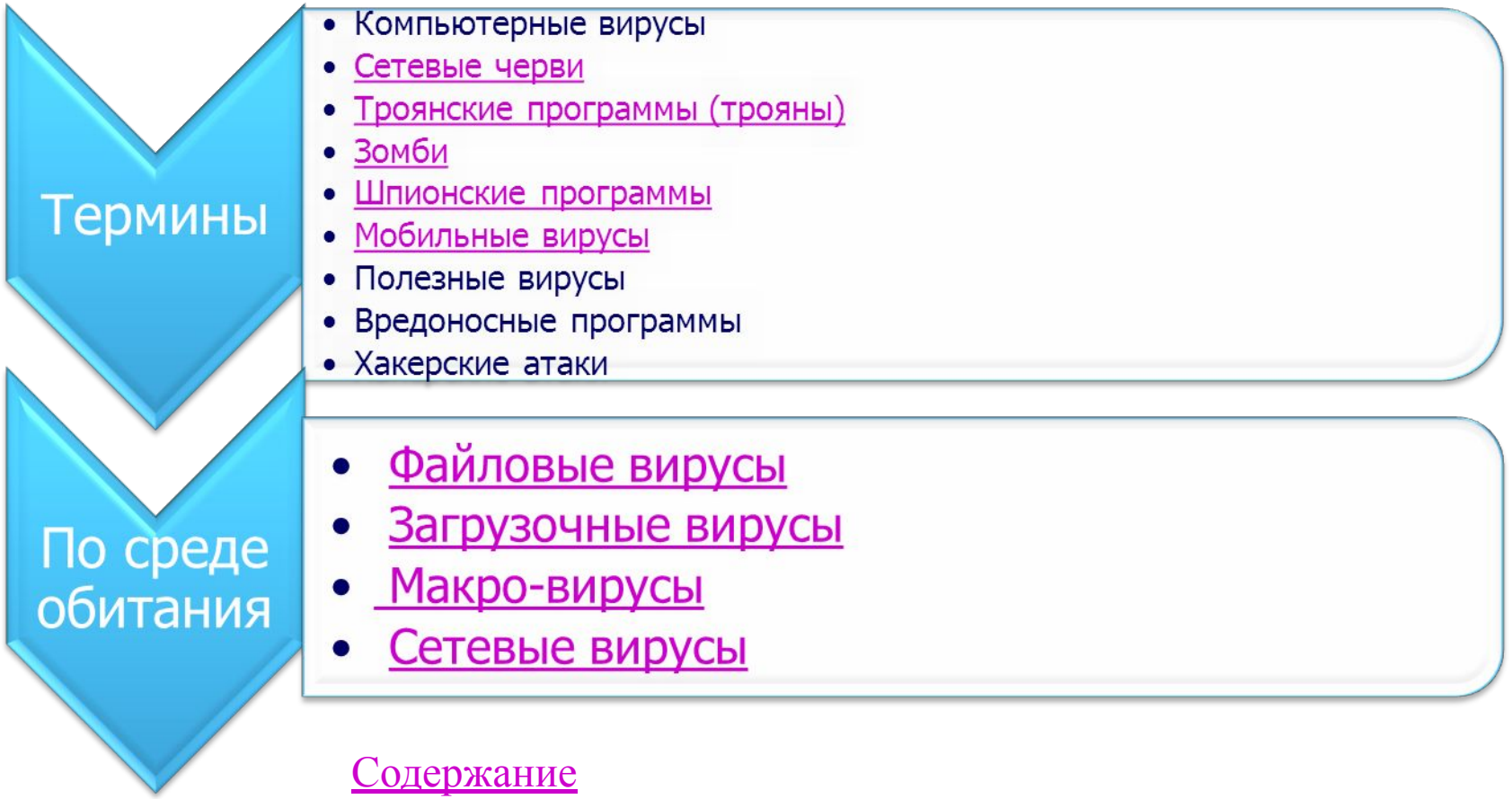
Сегодня миллионы российских пользователей Интернета становятся жертвами эпидемии «блокировщиков Windows».

По данным компании DrWeb, потери исчисляются сотнями миллионов рублей. Речь идет о вирусах, которые, заразив компьютер, блокируют Windows. Чтобы получить код для разблокировки, предлагается отправить SMS на короткий номер, после этого со счета абонента снимается от 300 до 600 рублей.

Содержание Назад

Типы компьютерных вирусов

В настоящее время не существует официальной классификации вирусов. Однако когда речь заходит о заражении или повреждении компьютера вирусами наиболее часто используется следующая терминология:



Содержание

Типы компьютерных вирусов

СЕТЕВЫЕ ЧЕРВИ

Червь (Worm) - *это программа, которая тиражируется на жестком диске, в памяти компьютера и распространяется по сети. Особенностью червей, отличающих их от других вирусов, 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.*

Типы компьютерных вирусов

ТРОЯНСКИЕ ПРОГРАММЫ

Троян или троянский конь (Trojans) - *это программа, которая находится внутри другой, как правило, абсолютно безобидной программы, при запуске которой в систему инсталлируются программа, написанная только с одной 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.*

Таким образом, троянские программы являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий.

Типы компьютерных вирусов

ЗОМБИ

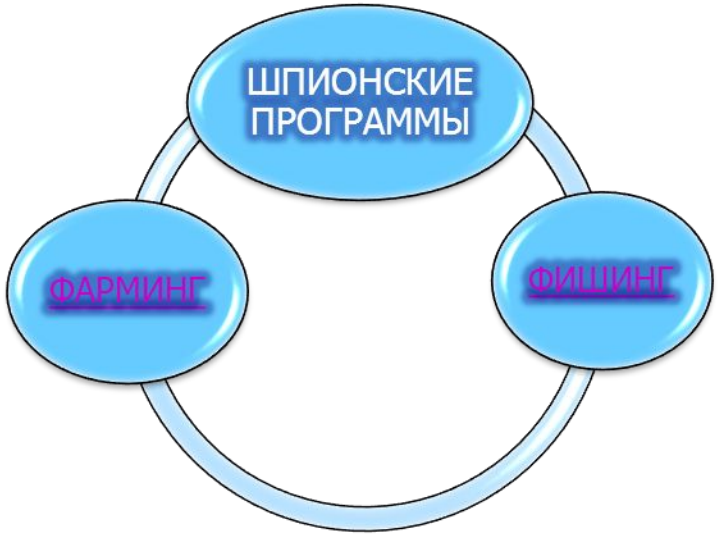
Зомби (Zombie) - *это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые рассылается огромное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

Типы компьютерных вирусов

ШПИОНСКИЕ ПРОГРАММЫ

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).



Содержание Назад Далее

Типы компьютерных вирусов

ШПИОНСКИЕ ПРОГРАММЫ (ФИШИНГ)

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.

ШПИОНСКИЕ ПРОГРАММЫ (ФАРМИНГ)

Фарминг – это 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.
Основной целью злоумышленников, использующих фарминг, является завладение личной финансовой информацией пользователя. Только вместо электронной почты мошенники используют более изощренные методы направления пользователя на фальшивый сайт.

Содержание Назад Далее

Типы компьютерных вирусов

МОБИЛЬНЫЕ ВИРУСЫ

Мобильные вирусы – *это компьютерные (программные) вирусы, разработанные злоумышленниками специально для распространения через мобильные устройства, такие как смартфоны и КПК. Чаще всего мобильные вирусы распространяются с помощью SMS и MMS сообщений, а также по каналу Bluetooth.*

Основной целью создания и распространения мобильных вирусов является несанкционированный доступ к личным данным владельцев сотовых телефонов и КПК, а также незаконное обогащение путем дистанционной организации звонков и рассылки SMS и MMS с чужих мобильных телефонов на платные номера. Наиболее известными и распространенными мобильными вирусами, в настоящее время являются: Cabir, Comwar, Brador, Viver и многие другие.

Типы компьютерных вирусов

ФАЙЛОВЫЕ ВИРУСЫ

Файловые вирусы *различными способами внедряются в исполнительные файлы, к которым относятся файлы с расширением *.exe, *.com и обычно активизируются при их запуске. После запуска зараженной программы вирус находится в оперативной памяти компьютера и является активным (т.е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.*
При этом файловые вирусы не могут заразить файлы данных.

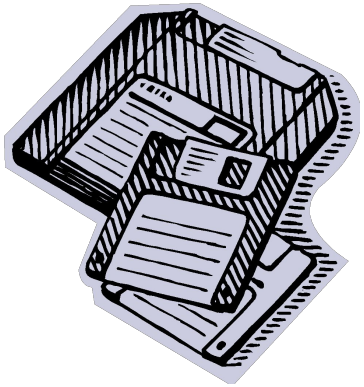
Содержание Назад Далее

Типы компьютерных вирусов

ЗАГРУЗОЧНЫЕ ВИРУСЫ

Загрузочные вирусы *записывают себя в загрузочный сектор диска. При загрузке операционной системы с зараженного диска вирусы внедряются в оперативную память. В дальнейшем загрузочный вирус ведет себя так же, как файловый, то есть может при обращении к ним компьютера.*

Вирус поражает загрузочный сектор жесткого диска и передается с компьютера на компьютер через зараженную дискету, если ее забыли вынуть из дисковода незараженного компьютера и перезагрузили этот компьютер.



Типы компьютерных вирусов

МАКРО-ВИРУСЫ

Макро-вирусы *заражают файлы документов Word и электронных таблиц Excel. Макро-вирусы являются фактически макрокомандами (макросами) После загрузки зараженного документа в приложение макро-вирусы присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается после закрытия приложения.*

Типы компьютерных вирусов

СЕТЕВЫЕ ВИРУСЫ

Распространяются по компьютерной сети и заражают при получении файлов с серверов файловых архивов. Существуют специфичные сетевые вирусы, которые используют для своего распространения электронную почту и Всемирную паутину.
Разновидностей сетевых вирусов очень много.

«Почтовые» вирусы	*Интернет - черви*	*Скрипт - вирусы*
Содержится во вложенных в почтовое сообщение файлах. Заражение компьютера происходит после открытия вложенного файла.	Распространяются в компьютерной сети во вложенных в почтовое сообщение файлах.	Передаются по Всемирной паутине в процессе загрузки Web-страниц с серверов в браузер локального компьютера

Содержание Назад

Методы защиты от компьютерных вирусов

1. Резервное копирование *всех программ, файлов и системных областей дисков на дискеты, чтобы можно было восстановить данные в случае вирусной атаки. Создание системной и аварийной дискеты.*
2. Ограничение доступа к машине *путем введения пароля, администратора, закрытых дисков.*
3. Включение антивирусного протектора *от загрузочных вирусов в CMOS Setup машины. Защита дискет от записи.*
4. Использование только лицензионного программного обеспечения, *а не пиратских копий, в которых могут находиться вирусы.*
5. Проверка всей поступающей извне информации *на вирусы, как на дискетах, CD-ROM, так и по сети.*
6. Применение антивирусных программ и обновление их версий.
7. Подготовка ремонтного набора дискет *(антивирусы и программы по обслуживанию дисков).*

Содержание

Антивирусные программы

ПОЛИФАГИ

РЕВИЗОРЫ

БЛОКИРОВЩИКИ

Содержание

Антивирусные программы

ПОЛИФАГИ

Принцип работы основан на проверке файлов, секторов дисков, оперативной памяти и поиске в них известных и новых вирусов. Полифаги могут обеспечить проверку файлов в процессе их загрузки в оперативную память. Такие программы называются антивирусными мониторами.

Достоинство полифагов: *универсальность.*

Недостаток: *небольшая скорость поиска вирусов.*

Примеры: *Kaspersky Anti-Virus, Dr.WEB.*

Содержание

Назад Далее

Антивирусные программы

РЕВИЗОРЫ

***П**ринцип работы основан на подсчете контрольных сумм для всех файлов на диске, которые сохраняются в базе данных антивируса. При последующем запуске ревизоры сверяют информацию записанную в базе данных с реальным значением, и если оно не совпадает, то ревизоры сигнализируют о том, что файл был изменен или заражен.*

Недостаток: ревизор не может обнаружить вирус в новых файлах (на дискетах, при распаковке файлов из архива, в электронной почте), поскольку в их базах данных отсутствует информация об этих файлах.

Пример: ADinf

Содержание Назад Далее

Антивирусные программы

БЛОКИРОВЩИКИ

Это программы, перехватывающие «вирусоопасные» ситуации (например, запись в загрузочный сектор дисков) и сообщающие об этом пользователю. Наибольшее распространение получили антивирусные блокировщики в BIOS компьютера. С помощью программы BIOS Setup можно провести настройку BIOS таким образом, что будет запрещена (заблокирована) любая запись в загрузочный сектор диска и компьютер будет защищен от заражения загрузочными вирусами.

Достоинства: *способность обнаруживать и останавливать вирус на самой ранней стадии его размножения.*

Содержание

Назад

Спасибо за внимание