МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Хакасский государственный университет им.
Н. Ф. Катанова»
Колледж педагогического образования, информатики и права

ПЦК естественнонаучных дисциплин, математики и информатики

РЕФЕРАТ

на тему:
Компьютерные вирусы

Автор реферата: _____ Каунова Д.М.
(подпись) (инициалы, фамилия)

Специальность: 09.02.03 - Программирование в компьютерных системах

Курс: II
Группа: И-21
Зачет/незачет:_____

Руководитель: _____ Когумбаева О.П.
(подпись, дата) (инициалы, фамилия)

г. Абакан, 2017 г.

Содержание

Введение

Вирус - специально написанная, как правило, небольшая по размерам программа, которая выполняет разрушительное действие на информационную часть компьютера. Вирус может размножаться, внедряясь в другие программы, в системную область диска и т.д.

Актуальность: Компьютер играет в жизни 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 из сети вирусы могут нарушить целостность и сохранность нашей информации.

Цели: определить, что является компьютерным вирусом и

ознакомиться с существующими методами защиты от компьютерных вирусов.

Задачи: выделить виды вирусов по способам проникновения их в компьютер и влиянию на работу и безопасность;

1. **Компьютерный вирус**

Компьютерный вирус— разновидность компьютерных программ или вредоносный код, отличительным признаком которых является способность к размножению (саморепликация).

Проникнув в компьютерную систему, вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае компьютерная система, пораженная вирусом, становится неработоспособной или же окажется под полным контролем злоумышленника.

Даже если автор вируса не программировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы обычно занимают некоторое место, иногда довольно значительное, в оперативной памяти или на накопителях информации и отбирают некоторые другие ресурсы системы. Поэтому вирусы относят к вредоносным программам.

1.1 Признаки заражения вирусом

При заражении компьютера вирусом важно его обнаружить, для этого следует знать основные признаки его проявления:

- 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 размера 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.

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера. Заразиться компьютерным вирусом можно только в определенных случаях:

- запуск на компьютере исполняемой программы, заражённой вирусом;

- загрузка компьютера с диска (дискеты), содержащего загрузочный вирус;

- подключение к системе заражённого драйвера;

- открытие документа, заражённого макровирусом;

- установка на компьютере заражённой операционной системы.

Компьютер не может быть заражён, если:

- на него переписывались текстовые и графические файлы (за исключением файлов, предусматривающих выполнение макрокоманд);

- на нём производилось копирование с одной дискеты на другую при условии, что ни один файл с дискет не запускался;

- на компьютере производится обработка принесённых извне текстовых и графических файлов, файлов данных и информационных файлов (за исключением файлов, предусматривающих выполнение макрокоманд);

- переписывание на компьютер заражённого вирусом файла ещё не означает заражения его вирусом. Чтобы заражение произошло нужно либо запустить заражённую программу, либо подключить заражённый драйвер, либо открыть заражённый документ (либо, естественно, загрузиться с заражённой дискеты). Иначе говоря, заразить свой компьютер можно только в том случае, если запустить на нём непроверенные программы и (или) программные продукты, установить непроверенные драйвера и (или) операционные системы, загрузиться с непроверенной системной дискеты или открыть непроверенные документы, подверженные заражению макровирусами.

2. Виды компьютерных вирусов

Компьютерные вирусы классифицируются по различным признакам. В зависимости от поведения их условно разделили на 6 категорий: по среде обитания, по особенностям строения кода, по способу заражения компьютера, по целостности, по возможностям, и дополнительно есть категория неклассифицируемых вирусов.

По среде обитания бывают следующие виды компьютерных вирусов:

- Сетевые - эти вирусы распространяются по локальным или глобальным сетям, заражая огромное количество компьютеров по всему миру.
- Файловые - внедряются в файл, заражая его. Опасность начинается в момент исполнения зараженного файла.
- Загрузочные - внедряются в загрузочный сектор жесткого диска и приступают к исполнению в момент загрузки системы.

По особенностям строения кода вирусы делят на:

- Паразиты - вирусы, которые, внедряясь в файлы, изменяют их содержимое по заданному алгоритму.
- Стелс, или невидимки, - вирусы, поражающие сектора жесткого диска, затем перехватывающие запросы операционной системы к этим секторам и перенаправляющие запрос на незараженные участки винчестера. Такие вирусы сложно обнаружить, отсюда и название.
- Полиморфные, или мутанты - это виды компьютерных вирусов, которые занимаются самокопированием, и при этом постоянно создают файлы с одним предназначением, но совершенно разным кодом.

По способу заражения кода вирусы делят на две группы:

- Резидентные - вредоносные программы, которые заражают оперативную память.
- Нерезидентные - вирусы, не заражающие оперативную память.

По целостности они делятся на:

- Распределенные - программы, разделенные на несколько файлов, но имеющие сценарий последовательности их исполнения.

- Целостные - единый блок программ, который выполняется прямым алгоритмом.

По возможностям предусмотрено деление вирусов на четыре следующие категории:

- Безвредные - виды компьютерных вирусов, способные замедлить работу компьютера путем своего размножения и поглощения свободного пространства на жестком диске.
- Неопасные - вирусы, которые замедляют работу компьютера, занимают значительный объем оперативной памяти и создают звуковые и графические эффекты.
- Опасные - вирусы, которые могут привести к серьезным системным сбоям, от зависания компьютера до разрушения операционной системы.
- Очень опасные - вирусы, способные стереть системную информацию, а также привести к физическому разрушению компьютера посредством нарушения распределения питания основных компонентов.

Разные вирусы, не попавшие под общую классификацию:

- Сетевые черви - вирусы, которые вычисляют адреса доступных компьютеров в сети и размножающиеся. Как правило, относятся к неопасным вирусам.
- Троянские программы, или трояны. Эти типы компьютерных вирусов получили свое название в честь знаменитого троянского коня. Эти вирусы маскируются под полезные программы. Предназначены в основном для хищения конфиденциальной информации, но есть и разновидности более опасных представителей вредоносного ПО.

2.1 **Механизм работы вирусов**

Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды

— например, пакетные файлы и документы MicrosoftWord и Excel, содержащие макросы. Кроме того, для проникновения на компьютер, вирус может использовать уязвимости в популярном программном обеспечении (например, AdobeFlash, InternetExplorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплоитом, использующим уязвимость.

2.2 Стадии жизни вируса

- из готового шаблона или «ручками», а также с помощью специальных KIT-ов прописывается код-тело вируса
- вирус дублируется на начальной стадии с течение некоторого времени на конкретных машинах жертвы, после этого инжектируется в сеть
- благодаря расхлябанности пользователей вирус получает распространение по сети, непрерывно заполняя незащищённые машины
- антивирусные программы отдельно друг от друга начинают распознавать вирус как вредоносное ПО и заносят данные по вирусу в свою БД
- благодаря своевременному обновлению антивирусного ПО, скорость распространения вируса снижается, инфицируемые машины избавляются от вредоносного кода и деятельность вируса сходит до минимума.

3. Вирус на компьютере

Вирусы способны быть незаметными, но в то же время выполнять нежелательные действия с компьютером. В одном случае присутствие вируса практически невозможно обнаружить, а в другом пользователь наблюдает ряд признаков заражения компьютера.

Антивирусные программы, или антивирусы, - это программные комплексы, имеющие обширные базы компьютерных вирусов, и выполняющие тщательную проверку жесткого диска на предмет наличия знакомых файлов или кода. Антивирусное ПО может вылечить, удалить или изолировать файл в специально отведенную область.

3.1 Способы распространения компьютерных вирусов

Способы распространения компьютерных вирусов разнообразны, однако существуют все же наиболее распространенные, от которых можно уберечься, соблюдая элементарные меры предосторожности.

Дискеты. Самый распространённый канал заражения в 1980-1990-е годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.

Флеш-накопители(флешки). В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, портативные цифровые плееры, а с 2000-х годов всё большую роль играют мобильные телефоны, особенно смартфоны (появились мобильные вирусы).

Электронная почта. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код.

Системы обмена мгновенными сообщениями. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

Веб-страницы. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов[4], ActiveX-компонент. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости вПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.

Интернет и локальные сети(черви).Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

Как видно, способов распространения компьютерных вирусов немало. Для предотвращения заражения необходимо соблюдать элементарные меры предосторожности:

стараться использовать только проверенные ресурсы в сети Интернет;

не скачивать сомнительные программы, а также не нажимать сомнительных картинок;

при получении писем от неизвестного адресата, обращать внимание на расширение приложенных файлов. Если они имеют такие типы

как:*.bat,*.vbs,*.scr,*.exe, то не стоит скачивать эти приложения, они могут быть заражены или попросту являются вирусом трояном;

применять лицензионные антивирусы. И тогда с легкостью можете избежать заражения.

4. Способы и методы защиты от вредоносных программ

Защита от компьютерных вирусов базируется на технических и организационных методах. Технические методы направлены на использование средств предотвращения вирусных угроз: антивирусы, брендмауэры, антиспамы и, конечно же, своевременное обновление операционной системы. Организационные - методы, которые описывают правильное поведение пользователя за компьютером с точки зрения информационной безопасности.

Технические методы предотвращают возможность проникновения вирусов на компьютер посредством программного обеспечения.

Антивирусы - контролируют файловую систему, неустанно проверяют и выискивают следы вредоносного кода. Брендмауэр предназначен для контроля за поступающей через сетевые каналы информацией и блокировки нежелательных пакетов.

Брендмауэр позволяет запретить определенный вид соединений по различным критериям: портам, протоколам, адресам и действиям.

Антиспамы - контролируют поступление нежелательной почты, и при поступлении в почтовый клиент подозрительного сообщения блокируют возможность исполнения вложенных файлов, пока пользователь не выполнит их принудительно. Бытует мнение, что антиспамы - самый неэффективный способ борьбы, однако ежедневно ими блокируются десятки миллионов писем с вложенными вирусами.

Обновление операционной системы - процесс, при котором разработчики исправляют ошибки и недочеты в работе ОС, использующиеся программистами для написания вирусов.

Организационные методы описывают правила работы за персональным компьютером, обработки информации, запуска и использования программного обеспечения, базирующиеся на четырех основных принципах:

1. Запускать и открывать только те документы и файлы, которые поступили из надежных источников, и в безопасности которых есть твердая

уверенность. При этом пользователь берет ответственность на себя, запуская ту или иную программу.

2. Проверять всю поступающую информацию из любых внешних источников, будь то Интернет, оптический диск или флеш-накопитель.

3. Всегда поддерживать в актуальном состоянии антивирусные базы и версию оболочки программного обеспечения по отлову и устранению угроз. Это обусловлено тем, что разработчики антивирусного ПО постоянно совершенствуют свои продукты, опираясь на появление новых вирусов;

4. Всегда соглашаться с предложениями антивирусных программ проверить флеш-накопитель или винчестер, подключенный к компьютеру.

4.1 Антивирусные программы

С появлением вирусов стали появляться программы, позволяющие их находить и обезвреживать. Ежедневно в мире появляются новые вирусы. Компьютерные продукты по их устранению обновляются по несколько раз в день, чтобы оставаться актуальными. Так, не затихая, идет постоянная борьба с компьютерными вирусами.

На сегодняшний день выбор антивирусных программ очень велик. На рынке то и дело появляются новые предложения, причем самые разнообразные: от полноценных программных комплексов до небольших подпрограмм, ориентированных только на один тип вирусов. Можно найти бесплатные или распространяющиеся по платной срочной лицензии решения безопасности.

Антивирусы хранят в своих базах сигнатур выдержки из кода огромного количества опасных для компьютерных систем объектов и во время проверки сравнивают коды документов и исполняемых файлов со своей базой. Если соответствие будет найдено, антивирус сообщит об этом пользователю и предложит один из вариантов обеспечения безопасности.

Компьютерные вирусы и антивирусные программы - неотъемлемые части друг друга. Бытует мнение, что ради коммерческой выгоды антивирусные программы самостоятельно разрабатывают опасные объекты.

Антивирусные программные утилиты делятся на несколько типов:

- Программы-детекторы. Предназначены для поиска объектов, зараженных одним из ныне известных компьютерных вирусов. Обычно детекторы только выискивают зараженные файлы, но в некоторых случаях способны заниматься лечением.
- Программы-ревизоры - эти программы запоминают состояние файловой системы, а спустя некоторое время проверяют и сверяют изменения. Если данные не соответствуют друг другу, программа проверяет, был ли подозрительный файл отредактирован пользователем. При отрицательном результате проверки пользователю выводится сообщение о возможном заражении объекта.
- Программы-лекари - предназначены для лечения программ и целых винчестеров.
- Программы-фильтры - выполняют проверку поступающей на компьютер извне информации и запрещают доступ подозрительным файлам. Как правило, выводят запрос пользователю. Программы-фильтры уже внедряются во все современные браузеры, чтобы своевременно найти компьютерный вирус. Это очень действенное решение, учитывающее сегодняшнюю степень развития Интернета.

Крупнейшие антивирусные комплексы содержат в себе все утилиты, которые объединены в один крупный защитный механизм. Яркими представителями антивирусного программного обеспечения на сегодняшний день являются: антивирус Касперского, Eset NOD32, Dr.Web, Norton Anti-Virus, Avira Antivir и Avast.

Эти программы обладают всеми основными возможностями, чтобы иметь право называться защитными программными комплексами. Некоторые из них имеют крайне ограниченные бесплатные версии, а некоторые предоставляются только за денежное вознаграждение.

4.2 Примеры антивирусных программ

Наиболее распространенные антивирусные программы: ADINF, AIDSTEST, AVP, DrWeb. NAV (Symantec), SCAN (McAfee), VIRUSAFE (Eliashim) и др. К антивирусам, которые зарекомендовали себя как достаточно надежные сканеры, можно отнести AVAST (Avil Software, Чехословакия), Dr.Solomon's AVTK ("Anti-Virus Toolkit", S&S International, Великобритания), NVC ("Norman Virus Control", Norman plc, Норвегия). Эти три программы вместе с AVP в последние годы показывают стабильно высокие результаты во всех антивирусных тестах. Неплохим сканером является также IBM Anti-Virus. За ними следуют F-PROT (Frisk Software, Исландия) и TBAV ("Thunderbyte Anti-Virus", ESaSS, Нидерланды). Эти две программы являются, пожалуй, наиболее мощными и популярными в мире shareware-сканерами. Нельзя не отметить антивирус SWEEP (Sophos plc, Великобритания).

Заключение

Таким образом, в этой работе я определила, что является компьютерным вирусом, ознакомилась с существующими методами защиты от них.

Так же выделила виды вирусов по способу проникновения их в компьютерную систему и влияние на ее работу и безопасность.

Узнала, как можно обезопасить свой компьютер от различных взломов, какими-либо программами. Возможно, на момент написания данной работы в мире появилась ещё пара-тройка новых, ещё более хитрых и совершенных вирусов. И ещё неизвестно, как с ними бороться. Проблема в том, что новые вирусы появляются чаще, чем разрабатываются антивирусные программы, впрочем, как и лекарства для человека. Вирусы очень умны, и их нельзя недооценивать. Лучше всего, как было сказано ранее, не ждать очередной вирусной атаки, а защитить себя от вирусов посредством специальных программ.

Библиографический список

1. Хаханов В.И. Модель неисправностей программного продукта. Компьютерный вирус. - 2-е изд.- 2013 г. - № 7. - С. 102. [Электронный ресурс] URL: http://cyberleninka.ru/article/n/model-neispravnosteyprogrammnogo-produkta-kompyuternyy-virus (дата обращения 22.01.2017)

2. Жуков Д.О. Модели различных стратегий распространения вирусов в компьютерных сетях. - 2013 г. - С. 113.[Электронный ресурс]: URL: http://cyberleninka.ru (дата обращения 22.01.2017)

3. Яцюк Т.В. Защита от вирусов-баннеров и вертуализаторов. - 2013 г. - № 9. - С. 122. [Электронный ресурс]: научная электронная библиотека. URL: http://cyberleninka.ru/article/n/zaschita-ot-virusov-banerov-i-osobennostiispolzovaniya-virtualizatorov (дата обращения 22.01.2017)

4. Блазуцкая Е.Ю., Шарафутдинов А.Г. Вирусы нового поколения и антивирусы. - 2015 г. Т. 1. № 35. С. 92-94. [Электронный ресурс]: URL: http://novainfo.ru/article/3754 (дата обращения 22.01.2017)

5. Абдуллин А.Р. Антивирусные программы - выбери лучший щит.- 2009 г. С. 258-259. [Электронный ресурс]: В сборнике: Студент и аграрная наука Материалы III Всероссийской студенческой конференции. URL: http://novainfo.ru/article/6504 (дата обращения 22.01.2017)

6. Абхалимова Р.С., Шарафутдинов А.Г. Информационные технологии xxi века научный журнал. Экономика и социум. - 2014 г. № 2-5 (11). С. 234-236.. [Электронный ресурс]: URL: http://www.iupr.ru/informacionnye_i_kommunikativnye_tehnologii__2_11__2014g_/ (дата обращения 22.01.2017)

7. Ханько В. В., Хаханов В. И., Фрадков С. А. Модель неисправностей программного продукта. Компьютерный вирус. - 1998 г. № 1. С. 99-101. [Электронный ресурс]:URL:http://cyberleninka.ru/article/n/modelneispravnostey-programmnogo-produkta-kompyuternyy-virus (дата обращения 22.01.2017)

8. Аханов В.В. Компьютерные вирусы. -1999 г. С. 15. [Электронный ресурс]:URL:http://helpcomputerblog.ru/kompyuternye-virusy/ (дата обращения 22.01.2017)

9. Сладко А.М. Компьютерные вирусы. Типы, виды, пути заражения. - 2015 г. С. 2. [Электронный ресурс]: URL:http://teralex.ru/bezrubriki/kompyuternye-virusy-tipy-vidy-puti-zarazheniya.html (дата обращения 22.01.2017)