МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ

ГАПОУ РБ «Бурятский республиканский многопрофильный техникум инновационных технологий»

ИНДИВИДУАЛЬНЫЙ ПРОЕКТ ПО ДИСЦИПЛИНЕ ИНФОРМАТИКА

РАЗНОВИДНОСТИ КОМПЬЮТЕРНЫХ ВИРУСОВ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ.

Выполнил обучающийся: **Адёнов Артур Бахетович**
(ФИО)

Группа: **БАС-17**
(наименование группы)

Специальность: **10.02.03 Информационная безопасность автоматизированных систем**
(наименование специальности)

Преподаватель: **Манжуева О. М.**
(фамилия, инициалы)

2018

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Компьютеры в наше время выполняют множество задач. Практически никто сейчас не работает без компьютера. Рынок IT процветает и развивается, появляются новые интернет-проекты и сервисы, люди все больше времени проводят в сети. Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

В связи с этим защита личной информации и нормальной работоспособности персональных компьютеров сейчас, как никогда, актуальна. Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных вредоносных программ.

Борьбой с компьютерными вирусами профессионально занимаются тысячи специалистов в десятках, а может быть, сотнях компаний, ведь именно компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации.

Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Актуальность исследования. 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.

Цель исследования. Выяснить пути проникновения и влияние вирусов на работу компьютера и определить методы защиты от них.

Задачи исследования:

1. Определить, что является компьютерным вирусом;

2. Выделить виды вирусов по способам проникновения их в компьютер и влиянию на работу и безопасность;

3. Ознакомиться с существующими методами защиты от компьютерных вирусов.

Объект исследования. Вредоносные программы.

Предмет исследования. Методы зашиты от вредоносных программ.

Практическая ценность. Моя работа может быть использована как дополнительный источник информация для объяснения понятия, что такое компьютерный вирус и как можно от него защититься.

Глава 1. ПОНЯТИЕ «КОМПЬЮТЕРНЫЙ ВИРУС»

Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения: процесс захвата компьютера вирусом полностью соответствует процессу захвата вирусом человеческого организма. Человеческий вирус внедряется в клетку, после чего начинает размножаться. Так и компьютерный: попав в программу, вирус действует аналогичным образом.

Считается, что впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом (GregoryBenford) в фантастическом рассказе «Человек в шрамах», опубликованном в журнале Venture в мае 1970 года.

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. Механизм работы компьютерных 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, использующий уязвимость.

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

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, ActiveX-компонент. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости ПО 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.

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:

1. Стараться использовать только проверенные ресурсы в сети Интернет;

2. Не скачивать сомнительные программы, а также не нажимать сомнительных картинок;

3. 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;

4. Применять лицензионные антивирусы.

И тогда с легкостью можете избежать заражения.

1.2. Признаки и случаи заражения

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.

Глава 2. КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

На сегодняшний день известны десятки тысяч различных вирусов. Несмотря на такое изобилие, число типов вирусов, отличающихся друг от друга механизмом распространения и принципом действия, весьма ограниченно. Существуют и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Таким образом, вирусы можно классифицировать по следующим признакам:

1. Среда обитания;
2. Способ заражения;
3. Степень воздействия;

Остановимся на них более подробно.

По среде обитания.

В зависимости от среды обитания вирусы делят на:

1. Сетевые – распространяются по различным компьютерным сетям;
2. Файловые - поражают файлы с расширением .com, .exe, реже .sys или оверлейные модули .exe файлов. Эти вирусы дописывают своё тело в начало, середину или конец файла и изменяют его таким образом, чтобы первыми получить управление. Получив управление, вирус может заразить другие программы, внедриться в оперативную память компьютера и т.д. Некоторые из этих вирусов не заботятся о сохранение заражаемого файла, в результате чего он оказывается неработоспособным и не подлежащим восстановлению;
3. Загрузочные - получают управление на этапе инициализации компьютера, еще до начала загрузки ОС. При заражении дискеты или жесткого диска загрузочный вирус заменяет загрузочную запись BR или главную загрузочную запись MBR. При начальной загрузке компьютера BIOS считывает загрузочную запись с диска или дискеты, в результате чего вирус получает управление еще до загрузки ОС. Затем он копирует себя в

конец оперативной памяти и перехватывает несколько функций BIOS. В конце процедуры заражения вирус загружает в память компьютера настоящий загрузочный сектор и передает ему управление. Далее все происходит, как обычно, но вирус уже находится в памяти и может контролировать работу всех программ и драйверов;

4. Файлово–загрузочные – комбинированные вирусы, объединяющие свойства файловых и загрузочных. В качестве примера можно привести широко распространенный когда-то файлово-загрузочный вирус OneHalf. Проникая в компьютер с ОС MS-DOS, этот вирус заражает главную загрузочную запись. Во время загрузки вирус постепенно шифрует секторы жесткого диска, начиная с самых последних секторов.

По способу заражения.

Резидентные вирусы — вирусы, которые при инфицировании компьютера оставляют свою резидентную часть в памяти. Они могут перехватывать прерывания операционной системы, а также обращения к инфицированным файлам со стороны программ и операционной системы. Эти вирусы могут оставаться активными вплоть до выключения или перезагрузки компьютера.

Нерезидентные вирусы — вирусы, не оставляющие своих резидентных частей в оперативной памяти компьютера. Некоторые вирусы оставляют в памяти некоторые свои фрагменты не способные к дальнейшему размножению такие вирусы считаются не резидентными.

По степени воздействия.

По степени воздействия вирусы можно разделить 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;

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

По особенностям алгоритма:

1. Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены;

2. Вирусы-невидимки (стелс-вирусы) – пытаются скрыть свое присутствие в компьютере. Если ОС или другая программа считывают файл зараженной программы, то вирус подставляет настоящий, незараженный, файл программы. Для этого резидентный модуль может временно удалять вирус из зараженного файла. После окончания работы с файлом он заражается снова. Загрузочные стелс-вирусы действуют по такой же схеме. Когда какая-либо программа считывает данные из загрузочного сектора, вместо зараженного подставляется настоящий загрузочный сектор.

3. Макрокомандные вирусы. Файлы документов MicrosoftOffice могут содержать в себе небольшие программы для обработки этих документов, составленные на языке VisualBasicforApplications. Это относится и к базам данных Access, а также к файлам презентаций PowerPoint. Такие программы создаются с использованием макрокоманд, поэтому вирусы, живущие в офисных документах, называются макрокомандными. Такие вирусы распространяются вместе с файлами документов. Чтобы заразить компьютер таким вирусом, достаточно просто открыть файл документа в соответствующем приложении. Распространенности данного вида вирусов в немалой степени способствует популярность MicrosoftOffice. Они могут изменять зараженные документы, оставаясь незамеченными долгое время.

Глава 3. ВИДЫ КОМПЬЮТЕРНЫХ ВИРУСОВ

Червь.

Червь – это самостоятельная программа, которая распространяется без участия пользователя. Если вирусы распространяются с помощью самих же пользователей, то черви делают это самостоятельно. Но они не заражают другие файлы, вместо этого они создают и распространяют копии самих же себя.

Некоторые черви распространяют свои копии через электронные письма. А другие не менее опасные и быстро распространяющиеся черви, используют сетевые уязвимости, вместо использования электронных писем. Они путешествуют по сети и заражают устаревшие и уязвимые системы в которых нет брандмауера.

Черви, которые распространяются по сети, могут генерировать большое количество трафика, замедляя при этом сеть. А после того, как он попадет в систему, он может выполнять те же действия что и вредоносный вирус.

Троян.

Троянская программа – эта программа полностью оправдывает свое название. Трояны названы в честь мифологического троянского коня. Чтобы покорить Трою, греки соорудили огромного деревянного коня и подарили его троянцам в качестве подарка. Троянцы приняли подарок в свой город. Позже, той ночью из деревянного коня вышли греческие воины и открыли ворота города — а что за этим последовало, вы можете себе представить.

Троянский конь — это примерно то же самое в компьютере. Троянский конь маскируется под полезные программы, т.е. выдает себя как нормальную и полезную программу, к примеру, такие программы как, руссификаторы, генераторы ключей и т.д. Попав в вашу систему, троян открывает бэкдор в вашей системе т.е. лазейку (уязвимость).

Затем, автор этого трояна будет использовать эту лазейку для своих целей. Например, он может использовать ваше интернет соединение для незаконных действий, которые в итоге будут указывать только на вас. Или для загрузки других вредоносных программ, в общем, через этот черный ход автор трояна может сделать все что угодно.

Программы шпионы.

Шпионы, чем-то похожи на троянские программы. Но у них есть главное отличие и заключается оно в том, что шпионы не наносят вреда файлам системы и пользователя. Шпионские программы по-тихому устраиваются на компьютере и шпионят. Они могут воровать пароли или даже сохранять абсолютно все что вы вводите с клавиатуры.

Программа шпион наиболее интеллектуальный тип вирусов и может даже отправлять файлы с зараженного компьютера. Шпион знает о зараженном ПК массу информации: какая система установлена, каким антивирусом вы пользуетесь, с какого браузера сидите в интернете, какие программы установлены на компьютере и так далее. Шпион – одна из самых опасных вредоносных программ.

Зомби.

Зомби — маленькие компьютерные программы, разносимые по сети Интернет компьютерными червями. Программы-зомби устанавливают себя в пораженной системе и ждут дальнейших команд к действию. Стандартные их действия - это зомбирование компьютеров.

Компьютер-зомби — компьютер в сети, используемый третьими лицами без ведома владельца, например для доступа в закрытую или коммерческую сеть, использования вычислительных ресурсов (кластеризации), рассылки спама, и т. п. Используются зомби-компьютеры также и с целями, с которыми используются открытые прокси. Данные компьютеры являются одним из наиболее эффективных инструментов по рассылке спама (50-80% мирового трафика спама).

Интернет-злоумышленники могут установить контроль над большим количеством компьютеров и использовать их в качестве зомби, которые образуют мощную сеть, осуществляющую вредоносную деятельность. Сети зомби, в которые могут входить до 100 000 компьютеров, используются для рассылки нежелательной почты, распространения вирусов, атак на другие компьютеры и серверы, а также совершения иных видов преступлений и мошенничества.

Сети зомби стали серьезной проблемой в Интернете.

Программы – блокировщики.

Программа-блокировщик (баннер) – эти программы блокируют доступ к операционной системе. При включении компьютера пользователь видит всплывающее окно, в котором обычно его в чем-то обвиняют: нарушении авторских прав или скачивании пиратского программного обеспечения. Далее, следуют угрозы полного удаления всей информации с компьютера. Для того чтобы этого избежать пользователь должен пополнить счет определенного телефона или отослать СМС. Только вот, даже если пользователь проделает все эти операции, баннер с угрозами никуда не денется.

Загрузочные вирусы.

Загрузочный вирус - компьютерный вирус, записывающийся в первый сектор гибкого или жесткого диска и выполняющийся при загрузке компьютера.

При включении или перезагрузки компьютера Boot-вирус заменяет собой загрузочный код, и таким образом получает управление ещё до непосредственного запуска операционной системы. Вместо операционной системы загружается вирус, размещая в памяти свое тело, которое хранит в неиспользованных секторах, идущих после MBR, но до первого загрузочного сектора раздела.

Перехватив обращения к дискам, вирус продолжает загрузку операционной системы. Размножается вирус записью в загрузочную область других накопителей компьютера.

Эксплоит.

Эксплойт («дыра в безопасности») – это компьютерная программа или скрипт, использующий недостатки или ошибки операционных систем и иного программного обеспечения. Одна из форм эксплойта – атаки из Интернет, реализованные при помощи манипулируемых пакетов данных, использующих «слабые места» в сетевом ПО. Таким образом в систему могут проникать программы, позволяющие получить повышенные права доступа.

«Удалённый эксплойт» работает через сеть и использует уязвимость в защите без какого-либо предварительного доступа к уязвимой системе. «Локальный эксплойт» требует предварительный доступ к уязвимой системе и обычно повышает привилегии для лица, запускающего эксплойт над уровнем, который был предоставлен системным администратором. Эксплойт «подставного сервера» подвергает риску машину конечного пользователя в том случае, когда к нему был совершён доступ с помощью уязвимого клиентского приложения. Эксплойт против клиентского приложения может также требовать некоторого взаимодействия с пользователем уязвимого приложения и может быть использован в связке с методами социальной инженерии.

Фарминг.

Фарминг – это перенаправление автоматически злоумышленниками пользователя Интернета на ложный сайт – правильную копию настоящего банка или сервисного торгового предприятия. Мошенники на компьютеры пользователей распространяют вредоносные программы, направленные на манипулирование файлом HOSTS или смену информации DNS. Пользователь способен получить данные вирусы на собственный компьютер, к примеру, открыв сторонний файл или письмо, посетив неправильный сайт.

Или, например, сообщение, что превышена максимально допустимая отсрочка платежа и счет заблокируют, с просьбой для более детального ознакомления прикрепленные документы открыть. Мошенническую схему активизируют, когда пользователь посещает сайт, который интересует преступников. В данный момент проходит переадресация обращения к официальному сайту пользователя на фальшивый, сделанный злоумышленниками для получения конфиденциальной информации специально. Не зная об обмане, жертва на сайте вводит запрашиваемые данные: пароли, номера счетов, ПИН-коды и прочие секретные данные, передавая их тем самым в руки преступников. В ситуациях с сервисными торговыми предприятиями по карте пользователя можно провести за не приобретаемые в действительности услуги и товары мошеннические транзакции.

Фишинг.

Фишинг - это способ получения мошенниками конфиденциальных данных пользователя: логина, пароля, кода, номера карт, счетов... Вид мошенничества связан с рассылкой сообщений и уведомлений от имени известных брендов, популярных серверов, банков, соцсетей. Целью мошенника является заполнение пользователем специальной формы с указанием своих данных или отправке их на определенный адрес. Для фишинга используются поддельные страницы временных сайтов, которые по форме и содержанию не отличаются от страниц сайта истинного владельца компании. Даже адрес фишинговой страницы может мало отличаться от реального.

Мошенники изощренными психологическими методами пытаются направить вас на свои поддельные страницы и под предлогом восстановления пароля или получения приза вынудить ввести логин и пароль, номер кошелька, счета и код. Все введенные вами данные сразу же будут переданы преступнику (записаны в лог файл или отправлены на его почту).

Как правило, фишинговые страницы не живут долго и постоянно меняют адреса сайтов. Это связано с тем, что производители основных браузеров, соц. почты и антивирусов легко определяют подобные страницы и уведомляют посетителей о подозрительном сайте или ссылке на него. Но у мошенников не занимает много времени заменять раз в 5-7 дней адреса сайтов.

Шпионское ПО.

Шпионское ПО, устанавливаясь скрытно, позволяет администраторам шпионить за пользователями либо лично контролировать персональный компьютер. Однако, название несет в себе более глубокий смысл нежели простой мониторинг деятельности пользователей.

Шпионские программы способны собирать различную личную информацию, например, данные интернет-серфинга либо информацию о посещенных сайтах. Данное ПО также помогает управлять компьютером, контролировать пользовательские задачи.

Вредоносные шпионы могут направлять поисковые запросы пользователя на незаконные сайты содержащие web-ловушки, вирусы. Помимо этого, незаконное шпионское ПО позволяет администраторам изменять настройки компьютера, приводя к замедлению процессов и возникновению ошибок, связанных с подключением к интернет-пространству.

Появление несанкционированных программ повлекло за собой создание антишпионского программного обеспечения, а также утверждение ряда законопроектов, связанных с гарантией безопасности электронных данных, в разных странах.

Руткит.

Руткит – это программа (набор программ) для скрытия следов присутствия злоумышленника или вредоносного кода в операционной системе. Установив руткит на ваш компьютер, хакер получает над ним полный контроль, может удаленно управлять компьютером и загружать на

него другие вредоносные программы. Естественно, все это он делает не вручную под покровом ночи, а пользуясь различными командами, утилитами и т.п.

Более того, основная задача руткита – не допустить обнаружения действий вирусов хозяином компьютера, скрыть от пользователя присутствие хакера и изменений в системе. Руткит прячет от ваших глаз вредоносные процессы, системные службы, драйвера, сетевые соединения, ключи реестра и записи автозагрузки, модули, папки, файлы и, конечно же, прячет сам себя. В общем, ситуация не из приятных, и ваш компьютер при этом могут использовать в любых не добрых целях.

Полиморфные вирусы.

Полиморфные вирусы - это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: защита от расшифровки. Имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку «по ходу дела», может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным. Полиморфные вирусы - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите. Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Программные вирусы.

Программные вирусы - это блоки программного кода, целенаправленно внедренные внутрь других прикладных программ. При запуске программы, несущей вирус, происходит запуск имплантированного в нее вирусного кода. Работа этого кода вызывает скрытые от пользователя изменения в файловой системе жестких дисков и/или в содержании других программ. Так, например, вирусный код может воспроизводить себя в теле других программ - этот процесс называется размножением. По прошествии определенного времени, создав достаточное количество копий, программный вирус может перейти к разрушительным действиям - нарушению работы программ и операционной системы, удалению информации, хранящейся на жестком диске. Этот процесс называется вирусной атакой. Самые разрушительные вирусы могут инициировать форматирование жестких дисков. Поскольку форматирование диска - достаточно продолжительный процесс, который не должен пройти незамеченным со стороны пользователя, во многих случаях программные вирусы ограничиваются уничтожением данных только в системных секторах жесткого диска, что эквивалентно потере таблиц файловой структуры. В этом случае данные на жестком диске остаются нетронутыми, но воспользоваться ими без применения специальных средств нельзя, поскольку неизвестно, какие сектора диска каким файлам принадлежит. Теоретически восстановить данные в этом случае можно, но трудоемкость этих работ исключительно высока.

Таким образом, можно сказать, что вредоносная программа – это любая программа, которая была создана для обеспечения доступа к компьютеру и хранящейся в нем информации без разрешения владельца этого самого компьютера. Целью таких действий является нанесение вреда или хищение какой-либо информации. Термин «Вредоносная программа» является обобщенным для всех существующих вирусов. Стоит помнить, что программа, которая была поражена вирусом уже не будет работать правильно. Поэтому ее нужно удалить, а затем установить заново.

Глава 4. ПРОФИЛАКТИКА И ЛЕЧЕНИЕ

Главным оружием в борьбе с вирусами являются антивирусные программы. Они позволяют не только обнаружить вирусы, но и удалить их из компьютера.

Итак, что же такое антивирус? Почему-то многие считают, что антивирус может обнаружить любой вирус, то есть, запустив антивирусную программу, можно быть абсолютно уверенным в их надежности. Такая точка зрения не совсем верна. Дело в том, что антивирус - это тоже программа, написанная профессионалом. Но эти программы способны распознавать и уничтожать только известные вирусы. То есть антивирус против конкретного вируса может быть написан только в том случае, когда у программиста есть в наличии хотя бы один экземпляр этого вируса. Но существует большое количество вирусов, алгоритм которых практически скопирован с алгоритма других вирусов.

Современные антивирусные технологии позволяют выявить практически все уже известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе. Кроме того, разработаны технологии моделирования поведения, позволяющие обнаруживать вновь создаваемые вирусные программы. Обнаруживаемые объекты могут подвергаться лечению, изолироваться (помещаться в карантин) или удаляться. Защита от вирусов может быть установлена на рабочие станции, файловые и почтовые сервера, межсетевые экраны, работающие под практически любой из распространенных операционных систем, на процессорах различных типов.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

Существует несколько основополагающих методов поиска вирусов, которые применяются антивирусными программамиДля обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов антивирусных программ:

1. Программы-детекторы;
2. Программы-доктора или фаги;
3. Программы-ревизоры (инспектора);
4. Программы-фильтры (мониторы);
5. Программы-вакцины или иммунизаторы;
6. Сканер;

Остановимся на них более подробно.

Программы-детекторы.

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов.

Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны". Некоторые программы-детекторы могут настраивать на новые типы вирусов, им необходимо лишь указать комбинации байтов, присущие этим вирусам. Тем не менее, невозможно разработать такую программу, которая могла бы обнаруживать любой заранее неизвестный вирус.

Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова - в ней могут сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, неизвестные программам-детекторам.

Большинство программ-детекторов имеют функцию "доктора", т.е. они пытаются вернуть зараженные файлы или области диска в их исходное

состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или удаляются.

Программы-доктора.

Программы-доктора (фаги). Фаг – это программа, которая способна не только обнаружить, но и уничтожить вирус, т.е. удалить его код из зараженных файлов и восстановить их работоспособность.

Очень мощными и эффективными антивирусными средствами являются фаги Doctor Web (созданный И. Даниловым) и KAV (автор Е. Касперский).

Детекторы этих фагов не просто сканируют файлы в поисках одной из известных вирусных сигнатур, но и реализуют эвристический метод поиска вирусов, могут находить и обезвреживать так называемые полиморфные вирусы, проверять файлы, находящиеся в архивах. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий.

Программы-ревизоры (инспектора).

Программы-ревизоры (CRC-сканеры) используют для поиска вирусов метод обнаружения изменений. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (кодов циклического контроля) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) затем сохраняются в БД антивируса. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в БД, с реально подсчитанными значениями. Если информация о файле, записанная в БД, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. Как правило, сравнение состояний производят сразу после загрузки ОС.

CRC-сканеры, использующие алгоритмы анти-стелс, являются довольно мощным средством против вирусов: практически 100 % вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у CRC-сканеров имеется недостаток, заметно снижающий их эффективность: они не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их БД отсутствует информация об этих файлах.

Программы - фильтры (мониторы).

Программы-фильтры – это «сторожа», которые постоянно находятся в ОП. Они являются резидентными и перехватывают все запросы к ОС на выполнение подозрительных действий, т. е. операций, которые используют вирусы для своего размножения и порчи информационных и программных ресурсов в компьютере, в том числе для переформатирования жесткого диска. Среди них можно выделить попытки изменения атрибутов файлов, коррекции исполняемых COM– или EXE-файлов, записи в загрузочные секторы диска.

При каждом запросе на подобное действие на экран компьютера поступает сообщение о том, какое действие затребовано, и какая программа будет его выполнять. В этом случае пользователь должен либо разрешить, либо запретить его исполнение. Постоянное нахождение программ-«сторожей» в ОП существенно уменьшает ее объем, что является основным недостатком этих программ. К тому же программы-фильтры не способны «лечить» файлы или диски. Эту функцию выполняют другие антивирусные программы, например AVP, Norton Antivirus for Windows, Thunder Byte Professional, McAfee Virus Scan.

Вакцины или иммунизаторы.

Вакцины или иммунизаторы - это резидентные программы, не допускающие заражение файлов. Вакцины используют в том случае, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация может

быть использована только от известных вирусов. Суть данного метода в том, что вакцина видоизменяет программу или диск таким образом, чтобы это не выражалось в их работе, а вирус будет считать их зараженными, и, следовательно, не внедрится. В настоящее время программы-вакцины ограничены в применении.

Иммунизаторы выделяются двух видов: иммунизаторы, оповещающие о заражении, и иммунизаторы, не допускающие заражение каким-либо вирусом. Первые чаще всего записываются в конце файлов и каждый раз при запуске файла проверяют его на изменение. Второй тип иммунизации охраняет систему от поражения вирусом какого-то определенного вида.

Сканер.

Программы-фаги (сканеры) используют для обнаружения вирусов метод сравнения с эталоном, метод эвристического анализа и некоторые другие методы. Программы-фаги осуществляют поиск характерной для конкретного вируса маски путем сканирования в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Программы-фаги не только находят зараженные вирусами файлы, но и «лечат» их, т. е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале работы программы-фаги сканируют оперативную память, обнаруживают вирусы и уничтожают их и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги — программы-фаги, предназначенные для поиска и уничтожения большого числа вирусов.

Программы-фаги можно разделить на две категории — универсальные и специализированные сканеры. Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от ОС, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов. Специализированные сканеры, рассчитанные только на

макровирусы, оказываются более удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Лицензионные антивирусные программы.

Выбор антивируса для домашнего пользования - актуальный вопрос, особенно для начинающих пользователей. Рано или поздно у любого возникает необходимость установки антивируса. Интересный факт, но многие пользователи вообще не устанавливают программ для защиты своего компьютера. Не устанавливают, пока не возникают различные сбои в работе системы. И действительно, при заражении компьютера вирусами замедляется работа системы, компьютер "тормозит" или "подвисает". В худшем же случае троянские программы могут похитить пароли и личную информацию. Как выбрать домашний антивирус, чтобы обезопасить себя от неприятностей попробуем разобраться.

Различные фирмы-производители программных продуктов, целенаправленно занимающиеся компьютерной и информационной безопасностью предлагают сегодня большой выбор антивирусных программ.

Приобретение лицензионной антивирусной программы обеспечит относительно надежную защиту данных от несанкционированного доступа и использования компьютера во вредоносных целях.

Глава 5. ОСНОВНЫЕ АНТИВИРУСНЫЕ ПРОГРАММЫ

NortonAntiVirus (Symantec).

Один из наиболее известных и популярных антивирусов, отлично зарекомендовал себя у пользователей по всему миру. В программе используется технология SONAR. позволяющая в режиме реального времени распознавать новые неизвестные вирусы. Данный антивирус не позволяет рассылать зараженные письма, автоматически распознает и блокирует вирусы, программы-шпионы и троянские компоненты, обнаруживает угрозы, скрытые в операционной системе, проверяет загружаемые файлы, выполняет функции просмотра электронной почты и защиты от интернет-червей.

Мастер по борьбе с вирусами выдает подробную информацию об обнаруженном вирусе, а также предоставляет вам возможность выбора: удалять вирус либо в автоматическом режиме, либо более осмотрительно, посредством пошаговой процедуры, которая позволяет увидеть каждое из выполняемых в процессе удаления действий.

Антивирусные базы обновляются очень часто (иногда обновления появляются несколько раз в неделю). Имеется резидентный монитор.

Антивирус Dr.Web(ЗАО «ДиалогНаука»).

Dr.Web - одна из самых известных и популярных отечественных антивирусных программ.

Имеет эвристический анализатор, позволяющий с большой долей вероятности обнаруживать неизвестные вирусы. При проверке какой-либо программы анализатор эмулирует ее исполнение и протоколирует все ее «подозрительные» действия, например, открытие или запись в файл, перехват векторов прерываний и т.д. На основе этого протокола принимается решение о возможном заражении программы вирусом.

Таким образом, с помощью эвристического анализатора кода обнаруживаются до 92% новых вирусов. Этот механизм достаточно эффективен и очень редко приводит к ложным срабатываниям. Файлы, в

которых эвристический анализатор обнаружил подозрение на вирус, называют возможно зараженными или подозрительными.

Dr.Web допускает автоматическую загрузку из Интернета новых баз данных вирусов и автообновление самой программы, что позволяет оперативно реагировать на появление новых вирусов. Передовые технологии Dr.Web позволяют организовать надежную антивирусную защиту, как в рамках крупных корпоративных сетей, так и на домашнем компьютере или в домашнем офисе. Антивирусные программы Dr.Web могут быть использованы практически под всеми популярными операционными системами.

Антивирусные программы Dr.Web отличаются от аналогичных решений других производителей исключительной нетребовательностью к ресурсам компьютера, компактностью, быстротой работы и надежностью в детектировании всех видов вредоносных программ.

Антивирус Касперского (ЗАО «Лаборатория Касперского»).

Антивирус Касперского – одна из популярнейших и наиболее качественных антивирусных программ. За счет специального алгоритма работы у нее очень высокий процент определения вирусов, в том числе и еще не известных. Антивирус Касперского умеет проверять на вирусы почтовые базы данных и получаемые письма вместе с приложениями к ним, очень хорошо определяет макровирусы, внедренные в документы Microsoft Office, а также проверяет наиболее популярные форматы архивов.

Основные функции:

1. Защита от вирусов, троянских программ и червей.
2. Защита от шпионского и рекламного ПО.
3. Проверка файлов, почты и интернет-трафика в режиме реального времени.
4. Защита от вирусов при работе с ICQ.
5. Защита от всех типов клавиатурных шпионов.

Возможность проверки архивов, даже вложенных. Следует отметить, что эта возможность является почти уникальной. Последняя версия программы может проверять содержимое архивов ZIP, ARJ, RAR. При проверке архивов, защищенных паролем, программа запрашивает этот пароль у пользователя.

Все подозрительные файлы (то есть те, для которых программа не смогла точно определить, заражен он или нет), размещаются в специальном разделе Карантин, в резервное хранилище программа записывает объекты, созданные во время антивирусной проверки.

Программа отлично справляется с контролем почтового трафика, контролируя всю отправляемую и принимаемую почту.

Ежедневное обновление базы вирусных сигнатур, автоматически реализуется через Интернет при помощи специально встроенного модуля и обеспечивает высокий уровень детектирования компьютерных вирусов.

Все это делает программу одной из лучших в своей категории.

Антивирус NOD32 (ESET, Словакия).

Очень быстро работающая антивирусная программа, эффективно защищающая от всех видов вирусов, включая троянские программы, черви, шпионские программы, рекламные программы, phishing-атаки. NOD32 обладает всеми возможностями, характерными для современных средств защиты компьютера, причем по некоторым очень важным параметрам NOD32 превосходит абсолютное большинство популярных антивирусных программ. Это единственный антивирус в мире, который уже более 10 лет не пропустил ни один активный на момент тестирования вирус, а также не менее мощный и встроенный виртуальный эмулятор для обнаружения полиморфных вирусов. Продукты NOD32предназначены как для защиты отдельных персональных компьютеров и рабочих станций, так и для защиты IT-инфраструктуры предприятий и организаций.

Panda Antivirus (Panda Software, Испания).

Panda Antivirus Pro 2011– мощный антивирус, включающий фаервол, защиту USB-устройств, загрузочный диск Panda SafeCD и набор инструментов для безопасного просмотра веб-сайтов. Благодаря технологиям Коллективного разума, этот антивирус стал еще более безопасным и быстрым, чем когда-либо, и предоставляет полную защиту от всех типов вредоносных программ.

Коллективный разум содержит серверы, которые автоматически классифицируют и обрабатывают информацию, поступающую от Сообщества пользователей и содержащую данные о вирусах, обнаруженных на их компьютерах. Персональный фаервол блокирует вторжения и атаки хакеров, даже если Вы работаете в своей беспроводной сети.

Panda USB Vaccine защищает Ваш ПК и USB-устройства от инфекций.

Panda SafeCD способен уничтожать на Вашем компьютере все типы вредоносных программ в случае, если Вы не можете запустить Windows. Он подсоединяется к Интернету для подключения самых современных антивирусных технологий каждый раз, когда это необходимо.

Avast! Free Antivirus (Чехия).

Бесплатный антивирус Avast!, работа которого основывается на отмеченном рядом наград антивирусном ядре, включает в себя все функции, которые необходимы профессиональной антивирусной программе. Он имеет простой пользовательский интерфейс, подходящий для новичков или неопытных пользователей. Последняя версия обеспечивает еще более высокую скорость сканирования и усовершенствованную функцию обнаружения вредоносных программ. В состав программы входит несколько работающих в реальном времени "экранов", которые наблюдает за всеми возможными опасными операциями, выполняемыми в течение ежедневной работы на компьютере, постоянно отслеживают вашу электронную почту и подключения к Интернету, проверяют файлы в вашем компьютере при каждом их открытии или закрытии.

После бесплатной регистрации на сайте программа будет работать один год, после чего опять потребуется регистрация. Программа полностью бесплатна для домашнего и некоммерческого использования.

AVG Anti-Virus Free 2011 (AVG Technologies, Чехия).

Эффективный и быстрый бесплатный антивирус. Гарантированные производителем быстрые обновления вирусной базы данных, простота использования, низкие системные требования – основные преимущества этого антивируса. AVG Anti-Virus Free Edition включает следующие компоненты: сканер, монитор, сканер электронной почты, систему автоматического обновления антивирусной базы.

Основные функции и возможности программы:

1. Проводит сканирование файлов во время их открытия и программ при их запуске;

2. Проверяет всю электронную почту;

3. Позволяет пользователю сканировать компьютер на наличие вирусов, как по расписанию, так и вручную;

4. Наличие системы автоматического обновления антивирусной базы;

5. Работает в фоновом режиме. Для выполнения задач программе требуется совсем немного системных ресурсов, поэтому в качестве антивируса она незаменима.

ЗАКЛЮЧЕНИЕ

Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение, а нарушение работы программно-аппаратных комплексов — удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей и т. п. — часто является его сопутствующей функцией. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

В обиходе «вирусами» называют всё вредоносное ПО, хотя на самом деле это лишь один его вид.

Все зависит от конкретного профиля рода занятий вирусов. Для одних главной задачей является предотвращение утечки информации к конкурентам. Другие могут уделять главное внимание целостности информации. Для третьих на первое место поднимается задача безотказной работы информационных систем (например, для провайдеров Интернет). Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека - в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

Из всего вышесказанного можно смело сделать вывод, что необходимость защиты от компьютерных вирусов на данный момент стоит на первом месте.

Для предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.

СПИСОК ИСТОЧНИКОВ ИНФОРМАЦИИ

1. Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов. – М.: «СОЛОН-Р», 2001.
2. Левин А.Ш. Самоучитель полезных программ. 4-е издание. – СПБ.: Питер, 2005.
3. Мостовой Д.Ю. Современные технологии борьбы с вирусами - Мир ПК. - №8. 2001.
4. Островский С. Компьютерные вирусы Информатика, январь 2002.
5. Безруков Н.Н. Классификация компьютерных вирусов MS-DOS и методы защиты от них/ Н.Н. Безруков. — М.: СП «ICE», 1990
6. Безруков Н.Н. Компьютерные вирусы/ Н.Н. Безруков. — М.: Наука, 1991.
7. Денисов Т.В. Антивирусная защита//Мой Компьютер-№4-1999.