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:

Изучение видов и характеристик компьютерных вирусов, а так же способы защиты от них.

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:

1. Изучить, что представляют собой компьютерные вирусы и как они распространяются.
2. Рассмотреть, какие существуют признаки заражения компьютера вирусом.
3. Изучить виды компьютерных вирусов и способы защиты от них.

1. История компьютерных вирусов

«Мнений по поводу рождения первого компьютерного вируса очень много. Нам доподлинно известно только одно: на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, вирусов не было, а в середине 1970-х годов они уже были. Несмотря на это, сама идея компьютерных вирусов появилась значительно раньше. Отправной точкой можно считать труды Джона фон Неймана по изучению самовоспроизводящихся математических автоматов, которые стали известны в 1940-х годах. В 1951 г. этот знаменитый ученый предложил метод, который демонстрировал возможность создания таких автоматов. Позднее, в 1959 г. журнал "Scientific American" опубликовал статью Л.С. Пенроуза, которая также была посвящена самовоспроизводящимся механическим структурам. В отличие от ранее известных работ, здесь была описана простейшая двумерная модель подобных структур, способных к активации, размножению, мутациям, захвату. Позднее, по следам этой статьи другой ученый Ф.Ж. Шталь реализовал модель на практике с помощью машинного кода на IBM 650.

Необходимо отметить, что с самого начала эти исследования были направлены отнюдь не на создание теоретической основы для будущего развития компьютерных вирусов. Наоборот, ученые стремились усовершенствовать мир, сделать его более приспособленным для жизни человека. Ведь именно эти труды легли в основу многих более поздних работ по робототехнике и искусственному интеллекту. И в том, что последующие поколения злоупотребили плодами технического прогресса, нет вины этих замечательных ученых.

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.

На этом теоретические исследования ученых и безобидные упражнения инженеров ушли в тень, и совсем скоро мир узнал, что теория саморазмножающихся структур с не меньшим успехом может быть применена и в несколько иных целях».

2. Классификация компьютерных вирусов

Нынче существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году)

2.1.Вирусы - программы

«Программные» вирусы, написанные для операционной системы Windows, решили эту проблему, маскируясь под разные «полезные» утилиты – например, под «ломалки» для условно-бесплатных программ или мультимедийные презентации. Другой излюбленный приём распространителей заразы – наряжать свои детища в «одежду» обновлений для операционной системы или даже… антивирусной программы! Увы, до сих пор многие пользователи, не задумываясь, запускают неизвестные программы, пришедшие в виде вложений в электронные письма якобы от Microsoft или «Лаборатории Касперского» - а ведь это самый верный путь поселить на свой компьютер вирус!

Большинство вирусов люди запускают на своём компьютере самостоятельно! – увы, несмотря на все усилия борцов с вирусами, некие стереотипы человеческой психологии оказываются непреодолимыми…

В 1995-1999 гг. на просторах Интернета весело развивалась добрая сотня «Windows-совместимых» вирусов. Эти милые зверушки, понятно, развились не просто так.… Только за период лета 1998 – лета 1999 г. Мир пережил несколько поистине разрушительных вирусных атак: в результате деятельности вируса Win95.CIH, поражающего BIOS системной платы, из строя были выведены около миллиона компьютеров во всех странах мира.

Сообщение об ошибке – результат работы вируса Blaster.

А совсем недавно, в середине 2003г., Сеть оказалась поражена новым «червем» SoBig, распространявшимся в виде вложения в электронные письма. Несмотря на то, что о вредоносных «вложениях» уже давно трубила вся пресса, люди запускали файл-вирус без малейших опасений. И вот результат: по данным аналитиков, в начале 2003 г. каждое 17-е письмо содержало в себе начинку в виде SoBig!

Впрочем, некоторые вирусы способны атаковать ваш компьютер даже в том случае, если его «тело» физически находится в другом месте. Например, один из самых «модных» вирусов 2003 г. – Blaster – был способен атаковать все компьютеры в локальной сети с одной-единственной машины! Сканируя локальную сеть, программа обнаруживала бреши в защите каждого компьютера, и самостоятельно пропихивала в эту «дырочку» вредоносный код.

Для борьбы с W32-вирусами одной антивирусной программы, увы, недостаточно – главным условием вашей безопасности является обязательная и регулярная загрузка обновлений к Windows. А именно – файлов-«заплаток», предназначенных для закрытия уже обнаруженных «дыр» в системе защите операционной системы.

Для получения новых «заплаток» вам необходимо навестить центр обновления Windows – сайт Windows Update (). При этом совершенно не обязательно набирать этот адрес в строке браузера вручную – достаточно зайти в меню Сервис программы Internet Explorer и выбрать пункт Windows Update.

На открывшейся страничке вы увидите полный список обновлений, доступных для загрузки. Учтите – все обновления из раздела «Критические обновления» необходимо устанавливать в обязательном порядке!

Посещайте сайт Windows Update не реже раза в месяц, регулярно обновляйте базы данных вашего антивирусного пакета – и можете считать, что от львиной доли неприятностей вы застрахованы…»2

2.2.**Загрузочные вирусы**

«Известные на текущий момент загрузочные вирусы заражают загрузочный (boot) сектор гибкого диска и boot-сектор или Master Boot Record (MBR)

винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера — после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает первый физический сектор загрузочного диска (A:, C: или CD-ROM в зависимости от параметров, установленных в BIOS Setup) и передает на него управление.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех описанных выше способах: вирус «заставляет» систему при ее перезапуске отдать управление не оригинальному коду загрузчика, а коду вируса.

Заражение дискет производится единственным известным способом — вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способами — вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в таблице разделов диска (Disk Partition Table), расположенной в MBR винчестера.

При инфицировании диска вирус в большинстве случаев переносит оригинальный boot-сектор (или MBR) в какой-либо другой сектор диска (например, в первый свободный). Если длина вируса больше длины сектора, то в заражаемый сектор помещается первая часть вируса, остальные части размещаются в других секторах (например, в первых свободных)»3

2.3.Файловые вирусы

«По способу заражения файлов вирусы делятся на: перезаписывающие (overwriting), паразитические (parasitic), вирусы-компаньоны (companion), вирусы-ссылки (link), вирусы, заражающие объектные модули (OBJ), вирусы, заражающие библиотеки компиляторов (LIB), вирусы, заражающие исходные тексты программ. Рассмотри некоторые из них.

Overwriting- данный метод заражения является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое.

Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

Parasitic – к паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.

Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (prepending), в конец файлов (appending) и в середину файлов (inserting). В свою очередь, внедрение вирусов в середину файлов происходит различными методами — путем переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла (cavity-вирусы).

Companion - к категории «companion» относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.

К вирусам данного типа относятся те из них, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл NOTEPAD.EXE переименовывается в NOTEPAD.EXD, а вирус записывается под именем NOTEPAD.EXE. При запуске управление получает код вируса, который затем запускает оригинальный NOTEPAD»4.

2.4.Полиморфные вирусы

«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.

Полиморфные вирусы - это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: 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»5.

2.5.Стелс-вирусы

«В ходе проверки компьютера антивирусные программы считывают данные - файлы и системные области с жестких дисков и дискет, пользуясь средствами операционной системы и базовой системы ввода/вывода BIOS. Ряд вирусов, после запуска оставляют в оперативной памяти компьютера специальные модули, перехватывающие обращение программ к дисковой подсистеме компьютера. Если такой модуль обнаруживает, что программа пытается прочитать зараженный файл или системную область диска, он на ходу подменяет читаемые данные, как будто вируса на диске нет.

Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными. Тем не менее, существует простой способ отключить механизм маскировки стелс-вирусов. Достаточно загрузить компьютер с не зараженной системной дискеты и сразу, не запуская других программ с диска компьютера (которые также могут оказаться зараженными), проверить компьютер антивирусной программой.

При загрузке с системной дискеты вирус не может получить управление и установить в оперативной памяти резидентный модуль, реализующий

стелсмеханизм. Антивирусная программа сможет прочитать информацию, действительно записанную на диске, и легко обнаружит вирус»6.

2.6.Макровирусы

В эпоху «классических» вирусов любой более-менее грамотный пользователь прекрасно знал: источником вирусной заразы могут быть только программы. И уж вряд ли даже в страшном сне могло присниться, что через несколько лет смертоносной начинкой обзаведутся… текстовые документы! Впрочем, такие сообщения время от времени проскакивали ещё в конце 80-х годов. Но появились они преимущественно первого апреля, так что никакой реакции, кроме смеха, вызвать не могли. Как оказалось, смеялись напрасно. В 1995 г., после появления операционной системы Windows 95 Microsoft с большой помпой объявила: старым DOS-вирусам конец, Windows защищена от них на 100%, ну а новых вирусов в ближайшее время не предвидится. Если бы! Уже в том же 1995 г. было зарегистрировано несколько мощных вирусных атак и создан первый вирус, работающий под Windows 95.

А меньше чем через полгода человечество было огорошено вирусами нового, совершенно неизвестного типа и принципа действия. В отличие от всех «приличных» вирусов, новички паразитировали не на исполняемых файлах, а на документах, подготовленных в популярных программах из комплекта Microsoft Office.

Ларчик открывался просто: в текстовый редактор Microsoft Word и таб¬личный редактор Microsoft Excel был встроен свой собственный язык про¬граммирования – Visual Basic for Applications (VBA), предназначенный для созданий специальных дополнений к редакторам – макросов. Эти макросы сохранялись в теле документов Microsoft Office и легко могли быть заменены вирусами. После открытия заражённого файла вирус активировался и заражал все документы Microsoft Office на вашем диске.

Первоначально макровирусы – а именно так называли новый класс вирусов, вели себя довольно пристойно. В крайнем случае – портили текстовые

документы. Однако уже в скором времени макровирусы перешли к своим обычным обязанностям – уничтожению информации.

3.Распространение

Через интернет, локальные сети и съемные носители.

3.1. Механизм

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 Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплоитом, использующим уязвимость.

3.2. Каналы

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). Использование этого канала ранее было преимущественно обусловлено возможностью создания на накопителе специального файла autorun.inf, в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. В Windows 7 возможность автозапуска файлов с переносных носителей была отключена.

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. Многие почтовые вирусы, попав на компьютер пользователя, затем используют адресную книгу из установленных почтовых клиентов типа Outlook для рассылки самого себя дальше.

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 в 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.

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.

4. Противодействие при обнаружении

Во времена MS-DOS были распространены стелс-вирусы, перехватывающие прерывания для обращения к операционной системе. Вирус таким образом мог скрывать свои файлы из дерева каталогов или подставлять вместо зараженного файла исходную копию.

С широким распространением антивирусных сканеров, проверяющих перед запуском любой код на наличие сигнатур или выполнение подозрительных действий, этой технологии стало недостаточно. Сокрытие вируса из списка процессов или дерева каталогов для того, чтобы не привлекать лишнее внимание пользователя, является базовым приемом, однако для борьбы с антивирусами требуются более изощренные методы. Для противодействия сканированию на наличие сигнатур применяется шифрование кода и полиморфизм. Эти техники часто применяются вместе, поскольку для расшифрования зашифрованной части вируса необходимо оставлять расшифровщик незашифрованным, что позволяет обнаруживать его по сигнатуре. Поэтому для изменения расшифровщика применяют полиморфизм — модификацию последовательности команд, не изменяющую выполняемых действий. Это возможно благодаря весьма разнообразной и гибкой системе команд процессоров Intel, в которой одно и то же элементарное действие, например, сложение двух чисел, может быть выполнено несколькими последовательностями команд.

Также применяется перемешивание кода, когда отдельные команды случайным образом разупорядочиваются и соединяются безусловными переходами. Передовым фронтом вирусных технологий считается метаморфизм, который часто путают с полиморфизмом. Расшифровщик полиморфного вируса относительно прост, его функция — расшифровать основное тело вируса после внедрения, то есть после того, как его код будет проверен антивирусом и запущен. Он не содержит самого полиморфного движка, который находится в зашифрованной части вируса и генерирует расшифровщик. В отличие от этого, метаморфный вирус может вообще не применять шифрование, поскольку сам при каждой репликации переписывает весь свой код.

4.1. Профилактика и лечение.

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)

- Не запускать незнакомые программы из сомнительных источников.

- Стараться блокировать возможность несанкционированного изменения системных файлов.

- Отключать потенциально опасный функционал системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).

- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.

- Пользоваться только доверенными дистрибутивами.

- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.

- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

4.2. Антивирусные программы

На сегодняшний день перечень доступных антивирусных программ весьма обширен. Они различаются как по цене (от весьма дорогих до абсолютно бесплатных), так и по своим функциональным возможностям. Наиболее мощные (и, как правило, более дорогие) антивирусные программы представляют собой пакеты специализированных утилит, способных при совместном их использовании поставить заслон практически любому виду вредоносных программ. Типовой перечень функций, которые способны выполнять антивирусные программы:

· сканирование памяти и содержимого дисков по расписанию;

· сканирование памяти компьютера, а также записываемых и читаемых файлов в реальном режиме времени с помощью резидентного модуля;

· выборочное сканирование файлов с измененными атрибутами;

· распознавание поведения, характерного для компьютерных вирусов;

· блокировка и/или удаление выявленных вирусов;

· восстановление зараженных информационных объектов;

· принудительная проверка подключенных к корпоративной сети компьютеров;

· удаленное обновление антивирусного программного обеспечения и баз данных с информацией о вирусах, в том числе автоматическое обновление баз данных по вирусам через Интернет;

· фильтрация трафика Интернета на предмет выявления вирусов в передаваемых программах и документах;

· выявление потенциально опасных Java-апплетов и модулей ActiveX;

· ведение протоколов, содержащих информацию о событиях, касающихся антивирусной защиты.

К наиболее мощным и популярным на сегодняшний день в России антивирусным пакетам относятся:

· Doctor Web (в документации часто именуется более кратко - Dr Web) программа российской компании;

· Антивирус Касперского (в документации именуется более кратко – AVP) разработка еще одной российской фирмы

· Norton AntiVirus корпорации Simantec;

· McAfee VirusScan компании Network Associates;

· Panda AntiVirus.

· Nod32 AntiVirus.

Популярность перечисленных выше пакетов обусловлена прежде всего тем, что в них реализован комплексный подход к борьбе с вредоносными

программами. То есть, установив такой пакет вы избавляетесь от необходимости использовать какие-либо дополнительные антивирусные средства.

Последние версии антивирусных пакетов содержат в своем составе также средства борьбы с вредоносными программами, проникающими из сети (в первую очередь из Интернета). Так какие же, собственно, существуют технологии выявления и нейтрализации компьютерных вирусов?

Специалисты в области антивирусной защиты выделяют пять типов антивирусов реализующих соответствующие технологии: сканеры, мониторы, ревизоры изменений, иммунизаторы и поведенческие блокираторы.

4.2.1.**Сканер**

Принцип работы антивирусного сканера состоит в том, что он просматривает файлы, оперативную память и загрузочные секторы дисков на предмет наличия вирусных масок, то есть уникального программного кода вируса. Вирусные маски (описания) известных вирусов содержатся в антивирусной базе данных сканера, и если он встречает программный код, совпадающий с одним из этих описаний, то выдает сообщение об обнаружении соответствующего вируса.

4.2.2.Программы-детекторы

Программы-детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти, на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные. Универсальные детекторы в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов. Специализированные детекторы выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы. Детектор, позволяющий обнаруживать несколько вирусов, называют полидетектором. Недостатком таких

антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

4.2.3.**Программы-доктора (фаги)**

Программы-доктора 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 своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

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

4.2.4.Программы-ревизоры

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем по желанию пользователя или периодически сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран видеомонитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс- вирусы и могут даже отличить изменения версии проверяемой программы от изменений внесенных вирусом.

4.2.5.Программы-филътры (сторожа)

Программы-фильтры представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

· попытки коррекции файлов с расширениями COM и EXE;

· изменения атрибутов файлов;

· прямая запись на диск по абсолютному адресу;

· запись в загрузочные сектора диска;

· загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако они не "лечат" файлы и диски. Для уничтожения вирусов требуются другие программы, например фаги. К недостаткам программ-сторожей можно отнести их назойливость (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим ПО.

4.2.6.Вакцины (иммунизаторы)

Вакцины - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, "лечащие" этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение. Существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

Заключение

Таким образом, в этой работе я определила, что является компьютерным вирусом, ознакомилась с существующими методами защиты от них. Так же выделила виды вирусов 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__2014 g_/ (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)