Содержание

Введение………………………………………………………………..…..3

1 Разновидности компьютерных вирусов………………………..………5

2 Методы защиты от компьютерных вирусов…………………………...9

3 Программы борьбы с компьютерными вирусами…………………….11

Заключение………………………………………………………………..15

Список реферируемой литературы……………………………………....16

Введение

С проникновением компьютеров в различные сферы жизни возникла принципиально новая отрасль – информационная индустрия. Объем циркулирующей в обществе информации примерно удваивается каждые пять лет. Человечество создало информационную цивилизацию, в которой от успешной работы средств обработки информации зависит само благополучие и даже выживание человечества и его нынешнем качестве. Произошедшие за этот период изменения можно охарактеризовать следующим образом:

- объемы обрабатываемой информации возросли за последние полвека на несколько порядков;

- информация приобрела стоимость, которую во многих случаях даже невозможно подсчитать;

- доступ к определенным данным позволяет контролировать значительные материальные и финансовые ценности;

- обрабатываемые данные стали чрезвычайно многообразными, а не исключительно текстовыми;

- субъектами информационных процессов теперь являются не только люди, но и созданные ими автоматизированные системы, действующие по заложенной в них программе.

В последние годы большое внимание уделяется вопросам защиты информации, накапливаемой, хранимой и обрабатываемой как в отдельных компьютерах, так и построенных на их основе вычислительных системах. При этом под защитой информации понимается создание совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации.

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

Проблема защиты информации специалистами интерпретируется следующим образом. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается ее уязвимость. Основными факторами, способствующими повышению этой уязвимости, являются:

- сосредоточие в единых базах данных информации различного назначения и принадлежности;

- резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы;

- расширение использования компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера.

Цель моего реферата: выяснить пути проникновения и влияние вирусов на работу компьютера и определить методы защиты от них.

Исходя из цели реферата, были сформулированы следующие задачи:

- определить, что является компьютерным вирусов;

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

- ознакомится с существующими методами защиты от компьютерных вирусов.

1 Разновидности компьютерных вирусов

Использование высокоэффективных информационных систем является обязательным условием успешной деятельности современных организаций и предприятий. Безопасность информации – это один из основных показателей качества информационной системы.

Одной из основных задач защиты информации является организация эффективной антивирусной защиты автономных рабочих станций, локальных и корпоративных компьютерных сетей, обрабатывающих информацию ограниченного доступа, а том числе содержащую государственную или служебную тайну.

Для обеспечения информационной безопасности используются программы, защищающие системы от компьютерных вирусов.

Вирус появился почти одновременно с появлением первых программ для компьютеров, и первоначально программы-вирусы писались не с целью наживы, а ради шуток над пользователями. Первая массовая эпидемия компьютерного вируса произошла в 1986 году, когда были заражены дискеты для первых массовых персональных компьютеров.

Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при её запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус, прежде всего, переписывает сам себя в другую рабочую программу и заражает её. После запуска программы, содержащей вирус, становится возможным заражение других файлов.

Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения .EXE, .COM, .SYS, .BAT. Редко заражаются текстовые файлы.

После заражения программы вирус может выполнить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания. И наконец, не забывает возвратить управление той программе, из которой он был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом заражается все программное обеспечение.

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;

- замедление работы компьютера;

- невозможность загрузки операционной системы;

- исчезновение файлов и каталогов или искажение их содержимого;

- изменение даты и времени модификации файлов;

- изменение размеров 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 [6], стр. 167 - 169.

Обязательным свойством компьютерного вируса является способность к размножению и незаметное для пользователя внедрение в файлы, загрузочные секторы дисков, документы. После заражения компьютера вирус может активизироваться и заставить компьютер выполнять какие-либо действия. Активизация вируса может быть связана с определенными действиями или событиями. Например, с наступлением определенной даты.

Компьютерный вирус – это основная реальная угроза информационной безопасности. Вирус – это разновидность вредоносных программ, отличительной особенностью которых является способность к размножению, к распространению с компьютера на компьютер и заражению целых компьютерных сетей.

И если раньше заражение происходило только при переносе вируса с одного компьютера на другой с помощью дискет, то теперь, благодаря доступности сети Интернет, подхватить вирус можно в один миг.

Программные вирусы – это блоки программного кода, которые внедряются в другие прикладные программы. Они имеют своим источником непроверенные программы с внешних носителей или программы, полученные из Интернета.

Загрузочные вирусы поражают системные области гибких и жестких дисков. На включенном компьютере они могут распространяться так же и в оперативную память.

Макровирусы – заражают файлы документов Word и электронных таблиц Excel. Заражение макровирусом происходит при открытии файла документа в окне программы.

Сетевые вирусы – обитают в компьютерных сетях Интернет – черви, которые распространяются в компьютерной сети во вложенных в почтовые сообщения файлы.

Файловые вирусы – внедряют свой код в исполняемые файлы – командные файлы, программы, драйвера.

Перезаписывающие вирусы – записывают свое тело вместо кода программы, не изменяя названия исполняемого файла. Вследствие этого исходная программа перестает запускаться. При загрузке программы выполняется код вируса, а не сама программа.

Вирусы-компаньоны – создают свою копию на месте заражаемой программы, но в отличие от перезаписываемых вирусов, не уничтожают оригинальный файл, а переименовывают или перемещают его. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе.

Вирусы-звенья – не изменяют кода программы, а заставляют операционную систему выполнять собственный код, изменяя адрес местоположения на диске зараженной программы на собственный адрес. После выполнения кода вируса управление обычно передается вызываемой пользователем программе.

Паразитические вирусы – это файловые вирусы, изменяющие содержание файла, добавляя в него свой код. При этом зараженная программа сохраняет полную или частичную работоспособность. Код может внедряться в начало, середину или конец программы. Код вируса выполняется перед, после или вместе с программой в зависимости от места внедрения вируса в программу.

С точки зрения безопасности работы электронной почты выделяют и другие виды угроз:

- утечка конфиденциальной информации;

- отказ в обслуживании;

- заражение компьютерным вирусом.

Утечка конфиденциальной информации является серьезной проблемой. Во избежание ее в почтовом обмене используют методы симметричной и несимметричной криптографии. Суть симметричной криптографии состоит в том, что обе стороны используют одинаковое шифрующее и дешифрующее программное обеспечение. Во втором случае отправитель шифрует сообщение с помощью сертификата (открытым ключом) получателя.

Электронная почта является благоприятной сферой для всех видов вирусов – как классических (которые распространяются в виде исполнимых файлов, вложенных в сообщения электронной почты), так и специфических почтовых вирусов [8], стр. 105 - 110.

2 Методы защиты от компьютерных вирусов

Для решения задач антивирусной защиты должен быть реализован комплекс известных и хорошо отработанных организационно-технических мероприятий:

- использование сертифицированного программного обеспечения;

- организация автономного испытательного стенда для проверки на вирусы нового программного обеспечения и данных. Предварительная проверка на автономном стенде нового программного обеспечения и данных позволяет значительно снизить вероятность проникновения в систему вирусов при ошибочных действиях пользователей. Это мероприятие эффективно для систем, обрабатывающих особо ценную информацию. Однако в случае эксплуатации компьютерной сети проверка на стенде входящих данных значительно снижает оперативность обработки информации;

- ограничение пользователей системы на ввод программ и данных с посторонних носителей информации. Отключение пользовательских дисководов для магнитных и оптических и оптических носителей информации, которые являются основным каналом проникновения вирусов в систему, позволяет значительно повысить уровень антивирусной защиты при работе в компьютерной сети;

- запрет на использование инструментальных средств для создания программ. Такой запрет необходим для того, чтобы исключить возможность создания пользователями вирусных программ в самой системе;

- резервное копирование рабочего программного обеспечения и данных. Правильная организация резервного копирования позволяет восстановить работоспособность системы и сохранить ценные данные в случае успешной вирусной атаки. Для критических систем рекомендуется циклическая схема тройного копирования данных, когда рабочая копия файла хранится на диске рабочей станции, одна архивная копия в защищенной области на сервере и еще одна архивная копия – на съемном носителе информации;

- криптографическое преобразование информации – является методом, повышающим безопасность передачи данных в сетях ЭВМ, данных, хранящихся в удаленных устройствах памяти, и при обмене информацией между удаленными объектами. Защита информации заключается в преобразовании ее составных частей (слов, букв, цифр и слогов) с помощью специальных алгоритмов и аппаратных решений. Управление процессом шифрования осуществляется с помощью периодически меняющегося кода ключа, обеспечивающего каждый раз оригинальное представление информации при использовании одного и того же алгоритма или устройства;

- подготовка администраторов безопасности и пользователей по вопросам антивирусной защиты. Низкая квалификация администраторов безопасности и пользователей по вопросам антивирусной защиты приводит к ошибочным действиям при настройке системы и в случае возникновения нештатных ситуаций. Обучение пользователей могут осуществлять специалисты службы защиты информации, прошедшие соответствующую подготовку в лицензированном учебном центре [6], стр. 341 - 345.

3 Программы борьбы с компьютерными вирусами

Широкое распространение компьютерных вирусов вызвало необходимость разработки антивирусных программ, позволяющих обнаруживать и уничтожать вирусы, «лечить» зараженные ресурсы.

Антивирусные программы могут использовать различные принципы для поиска и лечения зараженных файлов. Это:

- 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;

- программы-фильтры или сторожа (постоянно находятся в оперативной памяти компьютера и выполняют защитные функции. Они перехватывают все запросы к операционной системе на выполнение «подозрительных» действий);

- программы-ревизоры (предполагают подсчет контрольных сумм для присутствующих на диске файлов и сохранение их в базе данных антивируса. При последующем запуске ревизоры сверяют данные в базе данных с реально подсчитанными значениями сумм. Несовпадение значений свидетельствует о наличии заражения). Они запоминают исходное состояние программ, каталогов и т. д., когда компьютер еще не был заражен вирусом, а затем периодически сравнивают текущее состояние компьютера с исходным;

- программы-блокировщики (перехватывают вирусоопасные ситуации ситуации и сообщают об этом пользователю);

- программы-полифаги (проверяют файлы, загрузочные сектора дисков и оперативной памяти, осуществляют поиск в них известных и новых вирусов);

- программы-вакцины, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы неэффективны, т.к. ориентированы на очень узкую область.

Компьютерные сети имеют архитектурные особенности, которые оказывают влияние на уязвимость компьютерных систем при воздействии программных вирусов.

Основными из них являются:

- поддержка различных сетевых информационных услуг и удаленных пользователей;

- значительный объем информации между компьютерами;

Наличие различных платформ и протоколов взаимодействия;

- сложная конфигурация систем с большим количеством разнотипных узлов сети;

- использование информационных ресурсов публичных компьютерных сетей.

Полноту покрытия вирусного пространства проверяют в ходе тестовых испытаний, используя для этого коллекции:

- «живых» вирусов, составляющих набор примерно из 400 вирусов, которые встречаются на практике;

- макровирусов, поражающих в основном документы офисных приложений;

- полиморфных вирусов, меняющих свой код при генерации каждой новой копии;

- стандартных вирусов.

Периодически проводимые специализированными организациями испытания наиболее популярных антивирусных средств показывают, что они способны обнаруживать до 99,8% известных вирусов [7], стр. 475 - 479.

Наиболее широко используемыми антивирусными программами являются Антивирус Лаборатории Касперского, DRWeb, Norton Utilities и др.

Самыми популярными бесплатными программами являются:

- Антивирус BitDefenderFreeEdition – программа, которая поможет защитить систему, периодически проводя проверки и сканирование. При работе антивирус использует те же сертифицированные технологии обнаружения, что и платные продукты от BitDefender;

- AVG Anti-VirusFreeEdition 2013 из раздела бесплатных антивирусов позволит обеспечить базовую защиту компьютера. Хороший вариант для домашнего пользователя, который много времени проводит в социальных сетях благодаря встроенной функции защиты AVG SociaNetworkingProtection;

- Антивирус avast! FreeAntivirus – это один из лучших антивирусов среди бесплатных программ для защиты. Новое эвристическое ядро и высокая эффективность обнаружения сделали популярным avast среди пользователей всего мира;

- AviraFreeAntivirus – это антивирус от немецкого производителя, который обеспечивает надежную защиту, как от вирусов, так и от программ руткитов, использующих маскировку в своей работе;

- Comodo защитит систему от вирусов, шпионских программ, руткитов, а также от иных вредоносных программ. В антивирусе отсутствуют некоторые незначимые функции, поэтому он бесплатный. Имеется встроенная автоматическая функция песочница (AutoSandbox);

- Антивирус от Microsoft под названием SecurityEssentials предоставит защиту от вирусов, шпионов и других вредоносных программ. Наличие журнала проверки, планировщика, а также интуитивно понятный интерфейс, в также множество настроек;

- RisingAntivirusFreeEdition – это бесплатная программа для защиты системы, которая поможет как при ежедневной работе, так и при работе в сети Интернет. Антивирус имеет простой и удобный интерфейс, а также множество настроек;

- Zillya представлен на рынке украинскими экспертами по безопасности. Эвристическая проверка файлов, сканирование почты, большая антивирусная база и простой пользовательский интерфейс сделали этот довольно молодой антивирус популярным среди многих пользователей.

- Ad-Aware FREE InternetSecurity – это антивирус, который распространяется бесплатно и который сможет обеспечить полноценную защиту при работе в сети Интернет;

- PandaCloudAntivirus – это возможность использовать передовую защиту от Панда, ничего при этом не потратив. Антивирус оказывает минимальное воздействие на систему и обеспечивает максимальную защиту.

Если у вас нет времени или желания разбираться со всеми этими вопросами по выбору домашнего антивируса, то, основываясь на результаты тестов, проведенных авторитетными независимыми лабораториями можно выделить два лидера, которые подходят под понятие домашний антивирус. Эти антивирусы бесплатны, не нагружают систему, имеют высокую скорость сканирования и обеспечивают высокую степень защиты. Это антивирус Avast и антивирус Avira [4], стр. 280 - 284.

Заключение

Компьютерный вирус был назван по аналоги 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. Именно поэтому вирус считается самым страшным кошмаром любого пользователя сети Интернет, особенно который постоянно совершенствуется. Вирусы попадают на компьютеры часто, причем иногда не сразу понятно, что же произошло с системой.

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

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.

Таким образом задачи, поставленные при написании реферата выполнены, а цель работы достигнута полностью.

Список реферируемой литературы

1 Козлов Д. А. Энциклопедия компьютерных вирусов. – М.: «СОЛОН-Р», 2014. – 258 с.

2 Макарова Н. В. Информатика: Учебник для вузов. – СПб.: Питер, 2011. – 576 с.

3 Немцова Т. И. Практикум по информатике [Текст]: учеб.пособие / Т.И. Немцова, Ю.В. Назарова. - М.: ИНФРА-М,2008г. – 288 с.

4 Новиков М. Ю. Персональные компьютеры : аппаратура, системы, Интернет. Учебный курс [Текст] / Ю. Новиков , А. Черепанов . – СПб.: Питер, 2002 г. – 480 с.

5 Попов В.Б. Основы информационных и телекоммуникационных технологий. Мультемедия [Текст]: учебное пособие / В.Б.Попов. - М.: Финансы и статистика, 2007г. – 336 с.

6 Романова Ю. Д. Информатика и информационные технологии : учебное пособие. – 3-е изд., перераб. и доп. – М. : Эксмо, 2008. – 592 с.

7 Симонович С. В. Информатика. Базовый курс [Текст] / С. В. Симонович. – СПб.: Питер, 2013. – 640 с.

8 Хубаев Г. П. Информатика: учеб. пособие. – Изд. 3-е, перераб. и доп. – Ростов и/Д: Издательский центр «МарТ»; Феникс, 2010. – 288 с.