Содержание:

Введение

Мы живем на стыке двух тысячелетий, когда человечество вступило в эпоху новой научно-технической революции.

К концу двадцатого века люди овладели многими тайнами превращения вещества и энергии и сумели использовать эти знания для улучшения своей жизни. Но кроме вещества и энергии в жизни человека огромную роль играет еще одна составляющая - информация. Это самые разнообразные сведения, сообщения, известия, знания, умения.

В середине прошлого столетия появились специальные устройства - компьютеры, ориентированные на хранение и преобразование информации и произошла компьютерная революция.

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Информацией владеют и используют её все люди без исключения. Каждый человек решает для себя, какую информацию ему необходимо получить, какая информация не должна быть доступна другим и т.д. Человеку легко, хранить информацию, которая у него в голове, а как быть, если информация занесена в «мозг машины», к которой имеют доступ многие люди.

Многие знают, что существуют различные способы защиты информации. А от чего, и от кого её надо защищать? И как это правильно сделать?

То, что эти вопросы возникают, говорит о том, что тема в настоящее время актуальна. В курсовой работе я постарался ответить на эти вопросы, поставив перед собой

Цель: Выявление источников угрозы информации и определение способов защиты от них.

Задачи: Изучить уровень разработанности проблемы в литературе. Выявить основные источники угрозы информации. Описать способы защиты. Составить сравнительную таблицу антивирусных программ. Дать рекомендации по использованию этих программ.

Метод работы - анализ печатных изданий по данной теме. Анализ данных полученных методом сравнения.

Глава I Проблемы защиты информации человеком и обществом

- 1.

Использование информации

Информационные ресурсы в современном обществе играют не меньшую, а нередко и большую роль, чем ресурсы материальные. Знания, кому, когда и где продать товар, может цениться не меньше, чем собственно товар и в этом плане динамика развития общества свидетельствует о том, что на "весах" материальных и информационных ресурсов последние начинают превалировать, причем тем сильнее, чем более общество открыто, чем более развиты в нем средства коммуникации, чем большей информацией оно располагает.

С позиций рынка информация давно уже стала товаром, и это обстоятельство требует интенсивного развития практики, промышленности и теории компьютеризации общества. Компьютер как информационная среда не только позволил совершить качественный скачек в организации промышленности, науки и рынка, но он определил новые само ценные области производства: вычислительная техника, телекоммуникации, программные продукты.

Тенденции компьютеризации общества связаны с появлением новых профессий, связанных с вычислительной техникой, и различных категорий пользователей ЭВМ. Если в 60-70е годы в этой сфере доминировали специалисты по вычислительной технике (инженеры-электроники и программисты), создающие новые средства

вычислительной техники и новые пакеты прикладных программ, то сегодня интен сивно расширяется категория пользователей ЭВМ - представителей самых разных областей знаний, не являющихся специалистами по компьютерам в узком смысле, но умеющих использовать их для решения своих специфических задач.

Пользователь ЭВМ (или конечный пользователь) должен знать общие принципы организации информационных процессов в компьютерной среде, уметь выбрать нужные ему информационные системы и технические средства и быстро освоить их применительно к своей предметной области. Учитывая интенсивное развитие вычислительной техники и во многом насыщенность рынка программных продуктов, два последних качества приобретают особое значение.

- ○ 1.

Организация информации

хранение информации в памяти ЭВМ - одна из основных функций компьютера. Любая информация хранится с использованием особой символьной формы, которая использует бинарный (двоичный) набор изображающих знаков: (0 и 1). Выбор такой формы определяется реализацией аппаратуры ЭВМ (электронными схемами), составляющими схемотехнику компьютера, в основе которой лежит использование двоичного элемента хранения данных. Такой элемент (триггер) имеет два устойчивых состояния, условно обозначаемых как 1 (единица) и 0 (ноль), и способен хранить минимальную порцию информации, называемую бит (этот термин произведен от английского "binary digit" - двоичная цифра).

Понятие бита как минимальной единицы информации легко иллюстрируется простым примером. Допустим, Вы задаете собеседнику вопрос "Владеете ли Вы компьютерной грамотностью?", заранее точно зная, что он ответит "Да". Получаете ли Вы при этом, какую либо информацию? Нет, Вы остаетесь при своих знаниях, а Ваш вопрос в этой ситуации либо лишен всякого смысла, либо относится к риторическим.

Ситуация меняется, если Вы задаете тот же вопрос в ожидании получить один из двух возможных ответов: "Да" или "Нет". Задавая вопрос, Вы не владеете никакой информацией, т.е. находитесь в состоянии полной неопределенности. Получая ответ, Вы устраняете эту неопределенность и, следовательно, получаете информацию. Таким образом, двоичный набор возможных ответов, несущих

информацию, является минимальным. Следовательно, он определяет минимально возможную порцию получаемой информации.

Два бита несут информацию, достаточную для устранения неопределенности, заключающейся в двух вопросах при двоичной системе ответов и т.д.

преобразование информации из любой привычной нам формы (естественной формы) в форму хранения данных в компьютере (кодовую форму) связано с процессом кодирования. В общем случае этот процесс перехода от естественной формы к кодовой основан на изменении набора изображающих знаков (алфавита). Например, любой изображающий знак естественной формы (символ) хранится в памяти ЭВМ в виде кодовой комбинации из 8-ми бит, совокупность которых образует байт - основной элемент хранения данных в компьютере.

обратный процесс перехода от кодовой формы к естественной называется декодированием. Набор правил кодирования и декодирования определяет кодовую форму представления данных или просто код. (Разумеется, процессы кодирования, и декодирования в компьютере осуществляются автоматически без участия конечного пользователя).

Одни и те же данные могут быть представлены в компьютере в различных кодах и соответственно по-разному интерпретированы исполнительной системой компьютера.

Например, символ "1" (единица) может быть представлен в знаковой (символьной) кодовой форме, может быть представлен как целое число со знаком (+1) в коде целых чисел, как положительное целое без знака в коде кардинальных чисел, как вещественное число (1.) в коде вещественных чисел, как элемент логической информации (логическая единица - "истина") в коде представления логических данных. при этом любое из таких кодовых представлений связано

не только с собственным видом интерпретации, но и с различными кодовыми комбинациями, кодирующими единицу.

1.2 Угроза информации

1.2.1 Вирусы характеристика классификация

Можно привести массу фактов, свидетельствующих о том, что угроза информационному ресурсу возрастает с каждым днем, подвергая в панику ответственных лиц в банках, на предприятиях и в компаниях во всем мире. И угроза эта исходит от компьютерных вирусов, которые искажают или уничтожают жизненно важную, ценную информацию, что может привести не только к финансовым потерям, но и к человеческим жертвам.

Вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а, скажем, при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Разновидности вирусов устроены так, что при запуске зараженной программы вирус остается резидентно, т.е. до перезагрузки DOS, компьютера и время от времени заражает программы и выполняет вредные действия на компьютере.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющих в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Следует заметить, что тексты программ и документов, информационные файлы без данных, таблицы табличных процессоров и другие аналогичные файлы не могут быть заражены вирусом, он может их только испортить.

В настоящее время известно более 87800 вирусов, число которых непрерывно растет. Известны случаи, когда создавались учебные пособия, помогающие в написании вирусов.

Основные виды вирусов: загрузочные, файловые, файлово-загрузочные. Наиболее опасный вид вирусов - полиморфные. Из истории компьютерной вирусологии ясно, что любая оригинальная компьютерная разработка заставляет создателей антивирусов приспосабливаться к новым технологиям, постоянно усовершенствовать антивирусные программы.

Причины появления и распространения вирусов скрыты с одной стороны в психологии человека, с другой стороны - с отсутствием средств защиты у операционной системы.

Основные пути проникновения вирусов - съемные диски и компьютерные сети. Чтобы этого не случилось, соблюдайте меры по защите. Также для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов следствием не вполне ясного понимания предмета.

Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но, и могут вообще с ним не совпадать!

Вирус не может существовать в «полной изоляции»: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, т. е. В файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-c) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные. Резидентный вирус при заражении (инфицировании) компьютера оставляет в

оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

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

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. Известны вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые квазивирусные или «троянские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

ПРОЯВЛЕНИЕ НАЛИЧИЯ ВИРУСА В РАБОТЕ НА ПЭВМ

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметно. Однако по прошествии некоторого времени на компьютере начинает твориться что-то странное, например:

некоторые программы перестают работать или начинают работать неправильно;

на экран выводятся посторонние сообщения, символы и т.д.;

работа на компьютере существенно замедляется;

некоторые файлы оказываются испорченными и т.д.

К этому моменту, как правило, уже достаточно много (или даже большинство) программ являются зараженными вирусом, а некоторые файлы и диски - испорченными. Более того, зараженные программы с одного компьютера могли быть перенесены с помощью дискет или по локальной сети на другие компьютеры.

Некоторые виды вирусов ведут себя еще более коварно. Они вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, формируют весь жесткий диск на компьютере. А бывают вирусы, которые стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске компьютера.

Таким образом, если не предпринимать мер по защите от вируса, то последствия заражения компьютера могут быть очень серьезными.

РАЗНОВИДНОСТИ КОМПЬЮТЕРНЫХ ВИРУСОВ

Каждая конкретная разновидность вируса может заражать только один или два типа файлов. Чаще всего встречаются вирусы, заражающие исполнимые файлы. Некоторые вирусы заражают и файлы, и загрузочные области дисков. Вирусы, заражающие драйверы устройств, встречаются крайне редко, обычно такие вирусы умеют заражать и исполнимые файлы.

В последнее время получили распространение вирусы нового типа - вирусы, имеющие файловую систему на диске. Эти вирусы обычно называются DIR. T,

вирусы прячут свое тело в некоторый участок диска (обычно - в последний кластер диска) и помечают его в таблице размещения файлов (FAT) как конец файла.

Чтобы скрыть обнаружение, некоторые вирусы применяют довольно хитрые приемы маскировки. Я расскажу о двух из них: "невидимых" и самомодифицирующихся вирусах.

"НЕВИДИМЫЕ" вирусы. Многие резидентные вирусы (и файловые, и загрузочные) предотвращают свое обнаружение тем, что перехватывают обращения DOS (и тем самым прикладных программ) к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде. Разумеется, этот эффект наблюдается только на зараженном компьютере - на "чистом" компьютере изменения в файлах и загрузочных областях

диска можно легко обнаружить.

САМОМОДИФИЦИРУЮЩИЕСЯ вирусы. Другой способ, применяемый вирусами для того, чтобы укрыться от обнаружения, - модификация своего тела. Многие вирусы хранят большую часть своего тела в закодированном виде, чтобы с помощью дизассемблеров нельзя было разобраться в механизме их работы.

Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры этой кодировки, а кроме того, изменяют и свою стартовую часть, которая служит для раскодировки остальных команд вируса. Таким образом, в теле подобного вируса не имеется ни одной постоянной цепочки байтов, по которой можно было бы идентифицировать вирус. Это, естественно, затрудняет нахождение таких вирусов программами-детекторами.

1.2.2 Несанкционированный доступ

В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает и надежность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в нее изменений неуполномоченными лицами, и сохранение тайны переписки в электронной связи.

Разумеется, во всех цивилизованных странах на безопасности граждан стоят законы, но в вычислительные техники правоприменительная практика пока не развита, а законотворческий процесс не успевает за развитием технологий, и надежность работы компьютерных систем во многом опирается на меры

самозащиты.

1.2.3 Проблемы защиты информации Интернете

Internet - глобальная компьютерная сеть, охватывающая весь мир. Сегодня Internet имеет около 15 миллионов абонентов в более чем 150 странах мира. Ежемесячно размер сети увеличивается на 7-10%. Internet образует как бы ядро, обеспечивающее связь различных информационных сетей, принадлежащих различным учреждениям во всем мире, одна с другой.

Если ранее сеть использовалась исключительно в качестве среды передачи файлов и сообщений электронной почты, то сегодня решаются более сложные задачи распределенного доступа к ресурсам. Около двух лет назад были созданы оболочки, поддерживающие функции сетевого поиска и доступа к распределенным информационным ресурсам, электронным архивам.

Internet, служившая когда-то исключительно исследовательским и учебным группам, чьи интересы простирались вплоть до доступа к суперкомпьютерам, становится все более популярной в деловом мире.

Компании соблазняют быстрота, дешевая глобальная связь, удобство для проведения совместных работ, доступные программы, уникальная база данных сети Internet. Они рассматривают глобальную сеть как дополнение к своим собственным локальной сетям.

При низкой стоимости услуг (часто это только фиксированная ежемесячная плата за используемые линии или телефон) пользователи могут получить доступ к коммерческим и некоммерческим информационным службам США, Канады, Австралии и многих европейских стран. В архивах свободного доступа сети Internet можно найти информацию практически по всем сферам человеческой деятельности, начиная с новых научных открытий до прогноза погоды на завтра.

Internet и информационная безопасность несовместны по самой природе Internet. Она родилась как чисто корпоративная сеть, однако, в настоящее время с помощью единого стека протоколов TCP/IP и единого адресного пространства объединяет не только корпоративные и ведомственные сети (образовательные, государственные, коммерческие, военные и т.д.), являющиеся, по определению, сетями с ограниченным доступом, но и рядовых пользователей, которые имеют возможность

получить прямой доступ в Internet со своих домашних компьютеров с помощью модемов и телефонной сети общего пользования.

Как известно, чем проще доступ в Сеть, тем хуже ее информационная безопасность, поэтому с полным основанием можно сказать, что изначальная простота доступа в Internet - хуже воровства, так как пользователь может даже и не узнать, что у него были скопированы - файлы и программы, не говоря уже о возможности их порчи и корректировки.

Что же определяет бурный рост Internet, характеризующийся постоянным ростом числа пользователей? Ответ прост - «халява», то есть дешевизна программного обеспечения (TCP/IP), которое в настоящее время включено начиная с Windows 95, легкость и дешевизна доступа в Internet (либо с помощью IP-адреса, либо с помощью провайдера) и ко всем мировым информационным ресурсам.

Платой за пользование Internet является всеобщее снижение информационной безопасности, поэтому для предотвращения несанкционированного доступа к своим компьютерам все корпоративные и ведомственные сети, а также предприятия, использующие технологию intranet, ставят фильтры (fire-wall) между внутренней сетью и Internet, что фактически означает выход из единого адресного пространства. Еще большую безопасность даст отход от протокола TCP/IP и доступ в Internet через шлюзы.

Этот переход можно осуществлять одновременно с процессом построения всемирной информационной сети общего пользования, на базе использования сетевых компьютеров, которые с помощью сетевой карты и кабельного модема обеспечивают высокоскоростной доступ к локальному Web-серверу через сеть кабельного телевидения.

Для решения этих и других вопросов при переходе к новой архитектуре

Internet нужно предусмотреть следующее:

Во-первых, ликвидировать физическую связь между будущей Internet и корпоративными и ведомственными сетями, сохранив между ними лишь информационную связь через систему World Wide Web.

Во-вторых, заменить маршрутизаторы на коммутаторы, исключив обработку в узлах IP-протокола и заменив его на режим трансляции кадров Ethernet, при котором процесс коммутации сводится к простой операции сравнения MAC-адресов.

В-третьих, перейти в новое единое адресное пространство на базе физических адресов доступа к среде передачи (MAC-уровень), привязанное к географическому расположению сети, и позволяющее в рамках 48-бит создать адреса для более чем 64 триллионов независимых узлов.

Безопасность данных является одной из главных проблем в Internet. Появляются все новые и новые страшные истории о том, как компьютерные взломщики, использующие все более изощренные приемы, проникают в чужие базы данных. Разумеется, все это не способствует популярности Internet в деловых кругах. Одна только мысль о том, что какие-нибудь хулиганы или, что еще хуже, конкуренты, смогут получить доступ к архивам коммерческих данных, заставляет руководство корпораций отказываться от использования открытых информационных систем. Специалисты утверждают, что подобные опасения безосновательны, так как у компаний, имеющих доступ и к открытым, и частным сетям, практически равные шансы стать жертвами компьютерного террора.

Каждая организация, имеющая дело с какими бы то ни было ценностями, рано или поздно сталкивается с посягательством на них. Предусмотрительные начинают планировать защиту заранее, непредусмотрительные—после первого крупного “прокола”. Так или иначе, встает вопрос о том, что, как и от кого защищать. Обычно первая реакция на угрозу—стремление спрятать ценности в недоступное место и приставить к ним охрану. Это относительно несложно, если речь идет о таких ценностях, которые вам долго не понадобятся: убрали и забыли. Куда сложнее, если вам необходимо постоянно работать с ними. Каждое обращение в хранилище за вашими ценностями потребует выполнения особой процедуры, отнимет время и создаст дополнительные неудобства. Такова дилемма безопасности: приходится делать выбор между защищенностью вашего имущества и его доступностью для вас, а значит, и возможностью полезного использования.

Все это справедливо и в отношении информации. Например, база данных, содержащая конфиденциальные сведения, лишь тогда полностью защищена от посягательств, когда она находится на дисках, снятых с компьютера и убранных в охраняемое место. Как только вы установили эти диски в компьютер и начали использовать, появляется сразу несколько каналов, по которым злоумышленник, в принципе, имеет возможность получить к вашим тайнам доступ без вашего ведома. Иными словами, ваша информация либо недоступна для всех, включая и вас, либо не защищена на сто процентов.

Может показаться, что из этой ситуации нет выхода, но информационная безопасность сродни безопасности мореплавания: и то, и другое возможно лишь с учетом некоторой допустимой степени риска.

В области информации дилемма безопасности формулируется следующим образом: следует выбирать между защищенностью системы и ее открытостью. Правильнее, впрочем, говорить не о выборе, а о балансе, так как система, не обладающая свойством открытости, не может быть использована.

В банковской сфере проблема безопасности информации осложняется двумя факторами: во-первых, почти все ценности, с которыми имеет дело банк (кроме наличных денег и еще кое-чего), существуют лишь в виде той или иной информации. Во-вторых, банк не может существовать без связей с внешним миром: без клиентов, корреспондентов и т. п. При этом по внешним связям обязательно передается та самая информация, выражающая собой ценности, с которыми работает банк (либо сведения об этих ценностях и их движении, которые иногда стоят дороже самих ценностей). Извне приходят документы, по которым банк переводит деньги с одного счета на другой. Вовне банк передает распоряжения о движении средств по корреспондентским счетам, так что открытость банка задана, a priori.

Стоит отметить, что эти соображения справедливы по отношению не только к автоматизированным системам, но и к системам, построенным на традиционном бумажном документообороте и не использующим иных связей, кроме курьерской почты. Автоматизация добавила головной боли службам безопасности, а новые тенденции развития сферы банковских услуг, целиком, основанные на информационных технологиях, усугубляют проблему.

Глава II Сравнительный анализ и характеристики способов защиты информации.

2.1 Защита от вирусов

МЕТОДЫ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

общие средства защиты информации, которые полезны также и как страховка от порчи дисков, неправильно работающих программ или ошибочных действий пользователя;

профилактические меры, позволяющие уменьшить вероятность заражения вирусов;

специальные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

копирование информации - создание копий файлов и системных областей диска;

средства разграничения доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователя.

Общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

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". Программа Scan

McAfee Associates и Aidstest позволяют обнаруживать всего несколько тысяч вирусов, но всего их более 80 тысяч! Некоторые программы-детекторы, например, Norton AntiVirus или AVSP, 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.

Многие программы-детекторы (в том числе и Aidstest) не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Дело в том, что для чтения диска они используют функции DOS, перехватываются вирусом, который говорит, что все хорошо. Правда, Aidstest и др. программы могут выявить вирус путем просмотра оперативной памяти, но против некоторых "хитрых" вирусов это не помогает. Так что надежный диагноз программы-детекторы дают только при загрузке DOS с защищенной от записи дискеты, при этом копия программы-детектора также должна быть запущена с этой дискеты.

Некоторые детекторы, скажем, ADinf "Диалог-Наука", умеют ловить "невидимые" вирусы, даже когда они активны. Для этого они читают диск, не используя вызовы DOS. Этот метод работает не на всех дисководах.

Большинство программ-детекторов имеют функцию "доктора", т.е. пытаются вернуть зараженные файлы или области диска в их исходное состояние. Те файлы, которые не удалось восстановить, как правило, делаются неработоспособными или, удаляются.

Большинство программ-докторов умеют "лечить" только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам лечения новых вирусов.

К таким программам относится AVSP

"Диалог-МГУ".

ПРОГРАММЫ-РЕВИЗОРЫ имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Чтобы проверка состояния программ и дисков проходила при каждой загрузке операционной системы, необходимо включить команду запуска программы-ревизора в командный файл AUTOEXEC.BAT. Это позволяет обнаружить заражение компьютерным вирусом, когда он еще не успел нанести большого вреда. Более того, та же программа-ревизор сможет найти поврежденные вирусом файлы.

Многие программы-ревизоры являются довольно "интеллектуальными" - они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Понятно, что в нормальной ситуации такие изменения практически никогда не встречаются, поэтому программа-ревизор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они вызваны именно вирусом.

Следует заметить, что многие программы-ревизоры не умеют обнаруживать заражение "невидимыми" вирусами, если такой вирус активен в памяти компьютера. Но некоторые программы-ревизоры, например, ADinf фи "Диалог-Наука", все, же умеют делать это, не используя вызовы DOS для чтения диска (правда, они работают не на всех дисководах). Увы, против некоторых "хитрых" вирусов все это бесполезно.

Для проверки того, не изменился ли файл, некоторые программы-ревизоры проверяют длину файла. Но эта проверка недостаточна - некоторые вирусы не изменяют длину зараженных файлов. Более надежная проверка - прочесть весь файл и вычислить его контрольную сумму. Изменить файл так, чтобы его контрольная сумма осталась прежней, практически невозможно.

В последнее время появились очень полезные гибриды ревизоров и докторов, т.е. ДОКТОРА-РЕВИЗОРЫ - программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений

автоматически вернуть их в исходное состояние. Такие программы могут быть гораздо более универсальными, чем программы-доктора, поскольку при лечении они используют заранее сохраненную информацию о состоянии файлов и областей дисков. Это позволяет им вылечивать

файлы даже от тех вирусов, которые не были созданы на момент написания программы.

Но они могут лечить не от всех вирусов, а только от тех, которые используют "стандартные", известные на момент написания программы, механизмы заражения файлов.

Существуют также ПРОГРАММЫ-ФИЛЬТРЫ, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователя. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые программы-фильтры не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны – они позволяют обнаружить многие вирусы на самой ранней стадии, когда вирус еще не успел размножиться и что-либо испортить. Тем самым можно свести убытки от вируса к минимуму.

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 крайне неэффективны.

Защита информации в Интернете.

Сейчас вряд ли кому-то надо доказывать, что при подключении к Internet Вы подвергаете риску безопасность Вашей локальной сети и конфиденциальность содержащейся в ней информации. По данным CERT Coordination Center в 1995 году было зарегистрировано 2421 инцидентов - взломов локальных сетей и серверов. По результатам опроса, проведенного Computer Security Institute (CSI) среди 500 наиболее крупных организаций, компаний и университетов с 1991 число

незаконных вторжений возросло на 48.9 %, а потери, вызванные этими атаками, оцениваются в 66 млн. долларов США.

Одним из наиболее распространенных механизмов защиты от интернетовских бандитов - “хакеров” является применение межсетевых экранов - брандмауэров (firewalls).

Стоит отметить, что в следствии непрофессионализма администраторов и недостатков некоторых типов брандмауэров порядка 30% взломов совершается после установки защитных систем.

Не следует думать, что все изложенное выше - “заморские диковины”. Всем, кто еще не уверен, что Россия уверенно догоняет другие страны по числу взломов серверов и локальных сетей и принесенному ими ущербу, следует познакомиться с тематической подборкой материалов российской прессы и материалами Hack Zone (Zhurnal.Ru).

Не смотря на кажущийся правовой хаос в рассматриваемой области, любая деятельность по разработке, продаже и использованию средств защиты информации регулируется множеством законодательных и нормативных документов, а все используемые системы подлежат обязательной сертификации Государственной Технической Комиссией при президенте России.

- 1. Защита от несанкционированного доступа.

Известно, что алгоритмы защиты информации (прежде всего шифрования) можно реализовать как программным, так и аппаратным методом. Рассмотрим аппаратные шифраторы: почему они считаются более надежными и обеспечивающими лучшую защиту.

Что такое аппаратный шифратор.

Аппаратный шифратор по виду и по сути представляет собой обычное компьютерное «железо», чаще всего это плата расширения, вставляемая в разъем ISA или PCI системной платы ПК. Бывают и другие варианты, например, в виде USB ключа с криптографическими функциями, но мы здесь рассмотрим классический вариант - шифратор для шины PCI.

Использовать целую плату только для функций шифрования - непозволительная роскошь, поэтому производители аппаратных шифраторов обычно стараются насытить их различными дополнительными возможностями, среди которых:

1. Генерация случайных чисел. Это нужно, прежде всего, для получения криптографических ключей. Кроме того, многие алгоритмы защиты используют их и для других целей, например, алгоритм электронной подписи ГОСТ Р 34.10 - 2001. При каждом вычислении подписи ему необходимо новое случайное число.

2. Контроль входа на компьютер. При включении ПК устройство требует от пользователя ввести персональную информацию (например, вставить дискету с ключами). Работа будет разрешена только после того, как устройство опознает предъявленные ключи и сочтет их «своими». В противном случае придется разбирать системный блок и вынимать оттуда шифратор, чтобы загрузиться (однако, как известно, информация на ПК тоже может быть зашифрована).

3. Контроль целостности файлов операционной системы. Это не позволит злоумышленнику в ваше отсутствие изменить какие-либо данные. Шифратор хранит в себе список всех важных файлов с заранее рассчитанными для каждого контрольными суммами (или кэш значениями) и, если при следующей загрузке не совпадет эталонная сумма, хотя 6ы одного из них, компьютер будет 6локирован.

Плата со всеми перечисленными возможностями называется устройством криптографической защиты данных - УКЗД.

Шифратор, выполняющий контроль входа на ПК и проверяющий целостность операционной системы, называют также «электронным замком». Ясно, что аналогия неполная - обычные замки существенно уступают этим интеллектуальным устройствам. Понятно, что последним не обойтись без программного обеспечения - необходима утилита, с помощью которой формируются ключи для пользователей и ведется их список для распознавания «свой/чужой». Кроме этого, требуется приложение для выбора важных файлов и расчета их контрольных сумм. Эти программы обычно доступны только администратору по безопасности, который должен предварительно настроить все УКЗД для пользователей, а в случае возникновения проблем разбираться в их причинах.

Вообще, поставив на свой компьютер УКЗД, вы будете приятно удивлены уже при следующей загрузке: устройство проявится через несколько секунд после включения кнопки Power, как минимум, сообщив о себе и попросив ключи. Шифратор всегда перехватывает управление при загрузке IIK, после чего не так-то легко получить его обратно. УКЗД позволит продолжить загрузку только после всех своих проверок. Кстати, если IIK по какой-либо причине не отдаст управление

шифратору, тот, немного подождав, все равно его заблокирует. И это также прибавит работы администратору по безопасности.

Структура шифраторов.

Рассмотрим теперь, из чего должно состоять УКЗД, чтобы выполнять эти непростые функции:

1. Блок управления — основной модуль шифратора, который «заведует» работой всех остальных. Обычно реализуется на базе микро - контроллера, сейчас их предлагается немало и можно выбрать подходящий. Главное — быстродействие и достаточное количество внутренних ресурсов, а также внешних портов для подключения всех необходимых модулей.

2. Контроллер системной шины ПК. Через него осуществляется основной обмен данными между УКЗД и компьютером.

3. Энергонезависимое запоминающее устройство (ЗУ) — должно быть достаточно емким (несколько мегабайт) и допускать большое число треков записи. Здесь размещается программное обеспечение микроконтроллера, которое выполняется при инициализации устройства (т. е. когда шифратор перехватывает управление при загрузке компьютера).

4. Память журнала. Также представляет собой энергонезависимое ЗУ. Это действительно еще одна флэш-микросхема. Во избежание возможных коллизий память для программ и для журнала не должны объедимяться.

5. Шифропроцессор — это специализированная микросхема или микросхема программируемой логики. Собственно, он и шифрует данные.

6. Генератор случайных чисел. Обычно представляет собой такое устройство, дающее статистически случаиный и непредсказуемый сигнал- белый шум. Это может быть, например, шумовой диод

7. Блок ввода ключевой информации. Обеспечивает защищённый приём ключей с ключевого носителя, через него также вводится идентификационная информация о пользователе, необходимая для решения вопроса «свой\чужой».

8. Блок коммутаторов. Помимо перечисленных выше основных функций, УКЗД может по велению администратора безопасности ограничивать возможность работы с внешними устройствами: дисководами, CD-ROM и т.д.

Вывод

На мой взгляд, из всех отечественных программ, рассмотренных, здесь Dr.Web является самой полной, логически завершенной антивирусной системой. Остальные программы находятся, как бы в стадии развития. Программы-фаги, в принципе, не могут достигнуть логического завершения, так как должны развиваться, чтобы противостоять новым вирусам, хотя ADinf уже пошел по пути усовершенствования интерфейса. Высок потенциал у программы AVSP, которая при соответствующей доработке (упрощении алгоритмов поиска Stealth-вирусов, введении низкоуровневой защиты, улучшении интерфейса) может занять высокие позиции в среде антивирусов.

Заключение

В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает и надежность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в нее изменений неуполномоченными лицами, и сохранение тайны переписки в электронной связи. Разумеется, во всех цивилизованных странах на безопасности граждан стоят законы, но в вычислительной технике правоприменительная практика пока не развита, а законотворческий процесс не успевает за развитием технологий, и надежность работы компьютерных систем во многом опирается на меры самозащиты.

Итак, можно привести массу фактов, свидетельствующих о том, что угроза информационному ресурсу возрастает с каждым днем, подвергая в панику ответственных лиц в банках, на предприятиях и в компаниях во всем мире.

В процессе выполнения курсовой работы было проработано большое количество литературы, выявлены источники угрозы информации и определены способы защиты от них, была составлена сравнительная таблица антивирусных программ, даны рекомендации по использованию этих программ. Были исследованы 5 антивирусных программ, изучались их возможности в операционных средах MS-DOS и MS-Windows, методы настройки, режимы работы, а также простота функционирования. По результатам исследований для каждой антивирусной программы были даны рекомендации о возможности их использования в той или иной среде. На основании проведенных исследований можно сделать следующие

выводы. Для операционной среды MS-DOS и MS-Windows лучшей антивирусной программой является Dr.Web.

Список литературы

1. Информатика: Учебник / под ред. Проф. Н.В. Макаровой. - М.: Финансы и статистика, 1997.
2. Энциклопедия тайн и сенсаций / Подгот. текста Ю.Н. Петрова. - Мн.: Литература, 1996.
3. Безруков Н.Н. Компьютерные вирусы. - М.: Наука, 1991.
4. Мостовой Д.Ю. Современные технологии борьбы с вирусами // Мир ПК. - №8. - 1993.