

Практическая работа № 5

Антивирусные программы

Тема 3.6. Защита информации, антивирусная защита

Цель: Изучение технологии организации файлов с помощью программ – архиваторов.
Проверка информации на вирусную чистоту.

Ход работы:

1. Изучите команды и выполните предложенные упражнения:
2. Антивирусная проверка информации на диске.
3. Ответьте на контрольные вопросы и вопросы тестового задания.
4. Выполните задания практической работы.
5. Оформите отчет и сделайте вывод по практической работе.

Теоретический материал

Компьютерный 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 FAT-таблицу, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а 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.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющихся 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.

Признаки заражения компьютера вирусом

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.

Признаки заражения:

1. некоторые программы перестают работать или начинают работать неправильно;
2. на экран выводятся посторонние сообщения, символы и т.д.;
3. работа на компьютере существенно замедляется;
4. некоторые файлы оказываются испорченными и т.д.
5. операционная система не загружается;
6. изменение даты и времени модификации файлов;
7. изменение размеров файлов;
8. значительное увеличение количества файлов на диске;
9. существенное уменьшение размера свободной оперативной памяти и т.п.

Некоторые виды вирусов вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, форматируют весь жесткий диск на компьютере. Другие вирусы стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске.

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

Разновидности компьютерных вирусов

Вирусы классифицируют по среде обитания и по способу воздействия. По среде обитания вирусы подразделяются на следующие виды:

файловые вирусы, которые внедряются главным образом в исполняемые файлы, т.е. файлы с расширением exe, com, bat, но могут распространяться и через файлы документов;

загрузочные, которые внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска;

макровирусы, которые заражают файлы-документы и шаблоны документов Word и Excel.;

сетевые, распространяются по компьютерной сети;

По способу воздействия (особенностям алгоритма) вирусы отличаются большим разнообразием. Известны вирусы-паразиты, вирусы-черви, вирусы-невидимки (стелс-вирусы), вирусы-призраки (вирусы-мутанты), компаньон-вирусы, троянские кони и др.

Чаще всего встречаются вирусы, заражающие исполнимые файлы. Некоторые вирусы заражают и файлы, и загрузочные области дисков.

Чтобы предотвратить свое обнаружение, некоторые вирусы применяют довольно хитрые приемы маскировки. Рассмотрим "невидимые" и самомодифицирующиеся вирусы.

"Невидимые" вирусы. Многие **резидентные вирусы** (резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и

внедряется в них) (и файловые, и загрузочные) предотвращают свое обнаружение тем, что перехватывают обращения операционной системы 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.

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 физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;

профилактические меры, позволяющие уменьшить вероятность заражения вирусом;

специализированные 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 дисков;

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

Несмотря на то, что 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).

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. Такая комбинация называется **сигнатурой**. 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".

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.

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.

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.

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 пользователю. 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.

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.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Рассмотрим структуру этой обороны.

Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На переднем крае обороны находятся программы-фильтры. Эти программы могут первыми сообщить о работе вируса и предотвратить заражение программ и дисков.

Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры.

Самый глубокий эшелон обороны - это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные. В "стратегическом резерве" находятся архивные копии информации. Это позволяет восстановить информацию при её повреждении.

Итак, одним из основных методов борьбы с вирусами является своевременная профилактика их появления и распространения. Только комплексные профилактические меры защиты обеспечивают защиту от возможной потери информации. В комплекс таких мер входят:

Регулярное архивирование информации (создание резервных копий важных файлов и системных областей винчестера).

Использование только лицензионных дистрибутивных копий программных продуктов.

Систематическая проверка компьютера на наличие вирусов. Компьютер должен быть оснащен эффективным регулярно используемым и постоянно обновляемым пакетом антивирусных программ. Для обеспечения большей безопасности следует применять параллельно несколько антивирусных программ.

Осуществление входного контроля нового программного обеспечения, поступивших дискет. При переносе на компьютер файлов в архивированном виде после распаковки их также необходимо проверять.

При работе на других компьютерах всегда нужно защищать свои флэшки от записи в тех случаях, когда на них не планируется запись информации.

При поиске вирусов следует использовать заведомо чистую операционную систему, загруженную с диска.

При работе в сети необходимо использовать антивирусные программы для входного контроля всех файлов, получаемых из компьютерных сетей. Никогда не следует запускать непроверенные файлы, полученные по компьютерным сетям.

Современные технологии антивирусной защиты позволяют защитить от вируса файловые сервера, почтовые сервера и сервера приложений. Например, антивирус Касперского для защиты файловых серверов позволяет обнаружить и нейтрализовать все типы вредоносных программ на файловых серверах и серверах приложений.

В состав антивируса Касперского для защиты файловых серверов входят:

антивирусный сканер, осуществляющий антивирусную проверку всех доступных файловых систем на наличие вирусов по требованию пользователя. Проверяются в том числе архивированные и сжатые файлы;

антивирусный демон, являющийся разновидностью антивирусного сканера с оптимизированной процедурой загрузки антивирусных баз в память, осуществляет проверку данных в масштабе реального времени;

ревизор изменений, Kaspersky Inspector, отслеживает все изменения, происходящие в файловых системах компьютера. Модуль не требует обновлений антивирусной базы: контроль осуществляется на основе снятия контрольных сумм файлов (CRC – сумм) и их последующего сравнения с данными, полученными после изменения файлов.

Комбинированное использование этих модулей позволяет создать антивирусную защиту, наиболее точно отвечающую системным требованиям.

Обнаруженные подозрительные или инфицированные объекты могут быть помещены в предварительно указанную "карантинную" директорию для последующего анализа.

Антивирус Касперского обеспечивает полномасштабную централизованную антивирусную защиту почтовых систем, работающих под управлением ОС Solaris.

Проверке на наличие вирусов подвергаются все элементы электронного письма – тело, прикрепленные файлы (в том числе архивированные и компрессированные), внедренные OLE-объекты, сообщения любого уровня вложенности. Обнаруженные подозрительные или инфицированные объекты могут быть вылечены, удалены, переименованы, или помещены в заранее определенную карантинную директорию для последующего анализа.

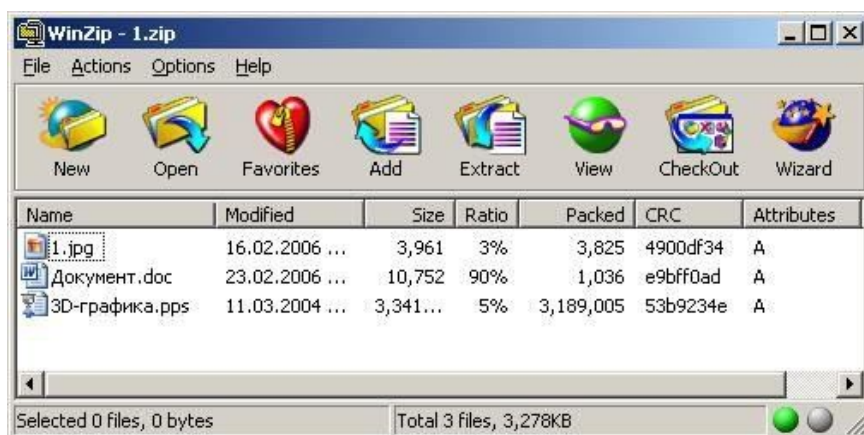
Ежедневное обновление базы вирусных сигнатур, автоматически реализуется через Интернет при помощи специально встроенного модуля и обеспечивает высокий уровень детектирования компьютерных вирусов.

Задание практической работы

Пройдите тест

Предлагаемые вопросы содержат несколько вариантов ответов. Выберите один или несколько правильных ответов.

1. Посмотрите на рисунок и выберите правильный ответ на вопрос: зависит ли степень сжатия от типа архивируемого файла?



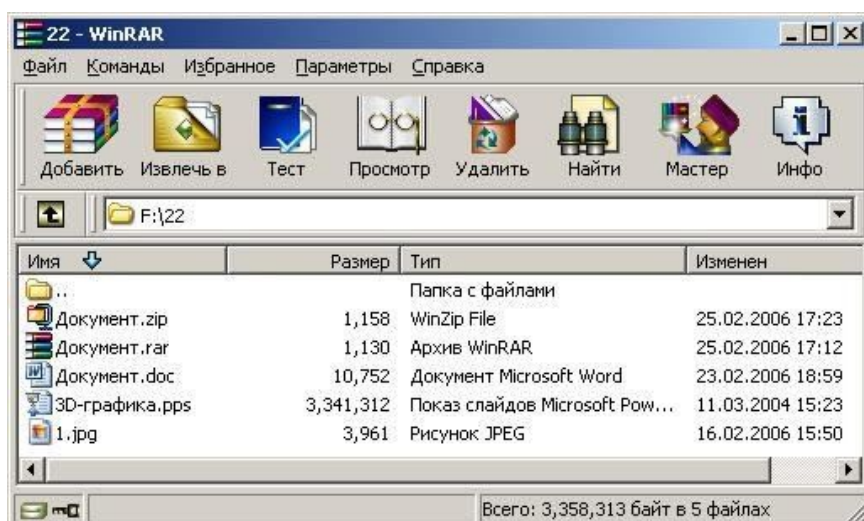
- a) да, зависит
- b) нет, не зависит

2. Посмотрите на рисунок и выберите правильный ответ на вопрос: какова примерно степень сжатия файла Документ.doc архиватором WinRar ?



- a) 3 %
- b) 10 %
- c) 100 %

3. Посмотрите на рисунок и выберите правильный ответ на вопрос: какой архиватор лучше сжал файл Документ.doc?



- a) WinRar
 - b) WinZip
 - c) Никакой разницы нет, степень сжатия одинакова.
4. Какие из перечисленных ниже действий могут привести к вирусной атаке?
- a) Создание нового документа.
 - b) Получение файла по электронной почте.
 - c) Установка на компьютер новой программы с пиратского диска.
 - d) Получение информации из Интернет.
5. Вирус – это...
- a) Ошибка в программе
 - b) Возбудитель инфекционного заболевания
 - c) Программа, обладающая способностью к самовоспроизведению.

Подготовьте письменное сообщение на тему: «Общие сведения и особенности работы антивирусной программы [*Название антивирусной программы*]» (Название антивирусной программы по указанию преподавателя).

№ п/п	Название антивирусной программы
1.	Dr.Web
2.	McAfee VirusScan
3.	Антивирус Касперского
4.	Panda Anti-Virus
5.	Avast!
6.	AVS
7.	AVG
8.	Avira
9.	Clam AntiVirus
10.	ClamWin
11.	NOD32
12.	Trojan Hunter
13.	VirusBuster
14.	Norton AntiVirus
15.	Windows Live OneCare
16.	PC-cillin
17.	F-Prot
18.	F-Secure Anti-Virus
19.	Comodo AntiVirus

Ответьте на контрольные вопросы:

Контрольные вопросы

1. Что называется компьютерным вирусом?
2. Какая программа называется "зараженной"?
3. Что происходит, когда зараженная программа начинает работу?

4. Как может маскироваться вирус?
5. Каковы признаки заражения вирусом?
6. Каковы последствия заражения компьютерным вирусом?
7. По каким признакам классифицируются компьютерные вирусы?
8. Как классифицируются вирусы по среде обитания?
9. Какие типы компьютерных вирусов выделяются по способу воздействия?
10. Что могут заразить вирусы?
11. Как маскируются "невидимые" вирусы?
12. Каковы особенности саомодифицирующихся вирусов?
13. Какие методы защиты от компьютерных вирусов можно использовать?
14. В каких случаях применяют специализированные программы защиты от компьютерных вирусов?
15. На какие виды можно подразделить программы защиты от компьютерных вирусов?
16. Как действуют программы-детекторы?
17. Что называется сигнатурой?
18. Всегда ли детектор распознает зараженную программу?
19. Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?
20. Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?
21. Перечислите меры защиты информации от компьютерных вирусов.
22. Каковы современные технологии антивирусной защиты?
23. Каковы возможности антивируса Касперского для защиты файловых серверов? почтовых серверов?
24. Какие модули входят в состав антивируса Касперского для защиты файловых систем?
25. Каково назначение этих модулей?
26. Какие элементы электронного письма подвергаются проверке на наличие вирусов?
27. Как обезвреживаются антивирусом Касперского обнаруженные подозрительные или инфицированные объекты?
28. Как обновляется база вирусных сигнатур?

Оформление результатов работы

1. Оформить работу в соответствии с заданиями.
2. Ответить на контрольные вопросы.
3. Сформулировать выводы по результатам работы.
4. Сдать и защитить работу.