**СОДЕРЖАНИЕ**

Введение 3

1. Антивирусная программа Aidstest 5

2. Антивирусная программа Doctor Web 7

3. Аппаратно-программный комплекс Sheriff 8

4. Антивирусный пакет AntiViral Toolkit Pro 9

Заключение 11

Список литературы 13

Введение

Единой классификации вирусов не существует, однако можно выделить три основные группы вирусов:

- файловые вирусы;

- загрузочные вирусы;

- комбинированные файлово-загрузочные вирусы.

Кроме того, вирусы бывают макрокомандные, резидентные и нерезидентные, полиморфные и маскирующиеся (стелс-вирусы).

Антивирусные программы. Существует несколько основных методов поиска вирусов, которые применяются антивирусными программами: сканирование; эвристический анализ; обнаружение изменений; резидентные мониторы. Антивирусы могут реализовывать все перечисленные выше методики, либо только некоторые из них.

Сканирование. Это наиболее традиционный метод поиска вирусов. Он заключается в поиске сигнатур, выделенных из ранyей обнаруженных вирусов. Антивирусные программы-сканеры, способные удалить обнаруженные вирусы, обычно называются полифагами. Сканеры могут обнаружить только уже известные и предварительно изученные вирусы, для которых была определена сигнатура. Поэтому программы-сканеры не защитят компьютер от проникновения новых вирусов, число которых постоянно увеличивается. Простые сканеры неспособны обнаружить и полиморфные вирусы, полностью меняющие свой код. Для этой цели необходимо использовать более сложные алгоритмы поиска, включающие эвристический анализ проверяемых программ.

Эвристический анализ. Этот метод нередко используется совместно со сканированием для поиска шифрующихся и полиморфных вирусов. Очень часто эвристический анализ позволяет обнаруживать ранее неизвестные инфекции, хотя лечение в этих случаях обычно оказывается невозможным. Если эвристический анализатор сообщает, что файл или загрузочный сектор, возможно, заражен вирусом, пользователю необходимо провести дополнительную проверку с помощью самых последних версий антивирусных программ- сканеров.

Обнаружение изменений. Заражая компьютер, вирус делает изменения на жестком диске: дописывает свой код в заражаемый файл, изменяет системные области диска и т.д. Антивирусные программы-ревизоры находят такие изменения: они запоминают характеристики всех областей диска, которые могут подвергаться нападению вируса, а затем периодически проверяют их и в случае обнаружения изменений выдают сообщение о подозрении на вирус. Следует учитывать, что не все изменения вызываются вторжением вирусов. Загрузочная запись может измениться при обновлении версии операционной системы, а некоторые программы записывают данные внутри своего исполняемого файла.

Резидентные мониторы. Антивирусные программы, постоянно находящиеся в оперативной памяти компьютера и отслеживающие все подозрительные действия, выполняемые другими программами, носят название резидентных мониторов, или сторожей. К сожалению, они имеют очень много недостатков: занимают много оперативной памяти и раздражают пользователей большим количеством сообщений, по большей части не имеющим отношения к проникновению вирусов.

Даже, если угрозы вирусов как будто бы нет, необходимо заранее провести мероприятия антивирусной защиты, в том числе организационного характера.

Для успешной борьбы с вирусами можно воспользоваться различными программными продуктами отечественного производства, некоторые из которых признаются лучшими в мире.

# 1. Антивирусная программа Aidstest

Антивирусная программа Aidstest (зарегистрированная торговая марка АО ДиалогНаука (DialogueScience), автор Лозинский Д.Н.). Программа Aidstest предназначена для обнаружения и исправления программ, зараженных определенными типами вирусов, а именно типами, известными в настоящее время автору. В комплект поставки входит несколько файлов. Перечень опознаваемых вирусов дается в файле aidsread.me, а их краткое описание - в файле aidsvir.txt, также поставляемом в комплекте с антивирусной программой. Этот набор вирусов постоянно пополняется по мере появления у автора новых вирусов. В процессе исправления программные файлы, которые исправить невозможно, стираются.

В момент запуска Aidstest в памяти не должно быть резидентных антивирусных программ, которые блокируют запись в программные файлы. Основной протокол Aidstest достаточно прост и понятен. Про каждый вирус, обнаруженный в файле, сообщается его имя, номинальная длина (в скобках после имени), а в случае успешного лечения через косую черту величина изменения длины файла (бывает и нулевой, если вирус при заражении не изменил длину файла). Программа обнаруживает и обезвреживает все известные ей типы вирусов и в памяти машины. В этом случае в конце работы на экран выдается предложение автоматически перезагрузить систему. Следует учитывать, что обезвреживание вирусов в памяти призвано, в первую очередь обеспечить возможность успешного завершения лечения. Некоторые функции системы при этом могут восстанавливаться неполноценно. Кроме того, свойства вирусов, не связанные с размножением, не убираются, т.е. может продолжаться осыпание букв, появление черного квадрата, исполнение мелодии и т.п.

Aidstest довольно надежно контролирует собственное здоровье относительно большинства типов вирусов. При обнаружении собственного заражения новым типом вируса Aidstest выдает соответствующее сообщение и прекращает работу.

Антивирусная программа Adinf. (зарегистрированная торговая марка АО ДиалогНаука (DialogueScience)). Поскольку Aidstest обнаруживает только уже известные автору вирусы, полезно иметь и программу, обнаруживающую появление на диске новых вирусов. АО ДиалогНаука предлагает один из эффективных и надежных ревизоров - ADinf Д.Мостового, который за несколько секунд просматривает весь диск и сообщает обо всех подозрительных происшествиях.

#

# 2. Антивирусная программа Doctor Web

Полиморфные вирусы, характерной особенностью которых является способность к существенной мутации своего кода, из-за чего программы типа Aidstest принципиально не в состоянии опознать (а значит, и обезвредить). Для борьбы с полиморфными вирусами следует использовать антивирус Doctor Web (автор И.Данилов), который благодаря встроенному эмулятору процессора опознает вирусы под различными шифровщиками и упаковщиками, а благодаря своему блоку эвристического анализа обнаруживает и многие (свыше 80%) неизвестные вирусы.

# 3. Аппаратно-программный комплекс Sheriff

Аппаратная защита позволяет защитить сами антивирусные средства от проникновения в них вирусов и рекомендуются для использования в особо ответственных случаях (банковско-финансовые учреждения, торговые предприятия и т.п.).

Norton AntiVirus for Windows 95 (Copiright Symantec). Пакет включает в себя резидентный мониторинг (Auto-Protect – автозащиту), сканер (Scanner), запускаемый вручную или периодически с помощью планировщика (Scheduler) и проверку при включении компьютера (StartUp) “критических” файлов (config, autoexec, command ит.п.).

Известные вирусы (порядка 6400 хранящихся в списке VirusList) могут быть обезврежены по мере их обнаружения, о новых вирусах выдается предупреждение. Во всех режимах работы может быть установлена обязательная проверка оперативной памяти (основной и расширенной), а также системных областей диска.

#

# 4. Антивирусный пакет AntiViral Toolkit Pro

Антивирусный пакет AntiViral Toolkit Pro (AVP) для Windows 95 (Windows NT) ЗАО “Лаборатория Касперского” является лучшей программа в своей области. Эта программа - новый шаг в борьбе с компьютерными вирусами. Она представляет из себя полностью 32-х разрядное приложение, оптимизированное для работы в популярной во всем мире среде Microsoft Windows 95 (Windows NT) и использующее все ее возможности. AVP имеет удобный пользовательский интерфейс, характерный для Windows 95, большое количество настроек, выбираемых пользователем, а также одну из самых больших в мире антивирусных баз (свыше 30000), что гарантирует надежную защиту от огромного числа самых разнообразных вирусов.

В ходе работы AVP сканирует: оперативную память (DOS, XMS, EMS), файлы, включая архивные и упакованные, системные сектора, содержащие Master Boot Record, загрузочный сектор (Boot-сектор) и таблицу разбиения диска (Partition Table).

Основные особенности AVP:

Детектирование и удаление огромного числа самых разнообразных вирусов, в том числе:

- полиморфных или самошифрующихся вирусов;

- стелс-вирусов или вирусов-невидимок;

- новых вирусов для Windows 3.XX и Windows 95;

- макро вирусов, заражающих документы Word и таблицы Excel.

Сканирование внутри упакованных файлов (модуль Unpacking Engine).

Сканирование внутри архивных файлов (модуль Extracting Engine).

Сканирование объектов на гибких, локальных, сетевых и CD-ROM дисках.

Эвристический модуль Code Analyzer, необходимый для детектирования неизвестных вирусов.

Поиск в режиме избыточного сканирования.

Проверка объектов на наличие в них изменений.

“AVP Monitor” – резидентный модуль, находящийся постоянно в оперативной памяти компьютера и отслеживающий все файловые операции в системе. Позволяет обнаружить и удалить вирус до момента реального заражения системы в целом.

# Заключение

Чтобы эффективно бороться с вирусами, необходимо иметь представление о “привычках” вирусов и ориентироваться в методах противодействия вирусам. Вирусом называется специально созданная программа, способная самостоятельно распространяться в компьютерной среде. Если вирус попал в компьютер вместе с одной из программ или с файлом документа, то через некоторое время другие программы или файлы на этом компьютере будут заражены. Если компьютер подключен к локальной или глобальной сети, то вирус может распространиться и дальше, на другие компьютеры. Авторы вирусных программ создают их из разных побуждений, однако результаты работы вирусов оказываются, как правило, схожими: инфекции портят программы и документы, находящиеся на компьютере, что часто приводит к их утрате. Некоторые вирусы способны уничтожать вообще всю информацию на дисках компьютеров, стоимость которой может в десятки и сотни раз превышать стоимость самого компьютера.

Внешние проявления деятельности вирусов весьма разнообразны. Одни вирусы относительно безопасны для данных и действуют только на нервы пользователю. Они могут, например, вызывать осыпание символов на экране, выводить на экран посторонние надписи, воспроизводить посторонние звуки через динамик компьютера. Другие - немного изменяют данные на диске компьютера. Этот случай наиболее опасен. Если пользователь вовремя не обнаружит вирус, и тот незаметно изменит файлы документов или баз данных, ошибка проявится позже в виде неправильных расчетов или искаженного баланса. Встречается вирус, выполняющий компрессию заражаемых файлов. Он сжимает файлы без разрешения пользователя.

Существует несколько основных методов поиска вирусов, которые применяются антивирусными программами: сканирование; эвристический анализ; обнаружение изменений; резидентные мониторы. Антивирусы могут реализовывать все перечисленные выше методики, либо только некоторые из них.

Для успешной борьбы с вирусами можно воспользоваться различными программными продуктами отечественного производства, некоторые из которых признаются лучшими в мире.

# Список литературы

1. Зверев В.С. Информатика: Учебное пособие для студентов вузов. Астрахань, 2003
2. Фигурнов А.Э. IBM-РС для пользователя. М., 1998
3. Компьютерные вирусы, виды и классификация//www.informatika.ru
4. www.kasperskylab.ru
5. www.web.ru
6. www.aidtest.ru
7. www.download.ru