Практическая работа № 2

Обнаружение вируса и устранение последствий его влияния
1. Цель работы

Целью работы является изучение методов обнаружения вирусов и методов удаления последствий заражения вирусами с использованием антивирусной утилиты AVZ.

2. Теоретические сведения

Массовое распространение вирусов, серьезность последствий их воздействия на ресурсы КС вызвали необходимость разработки и использования специальных антивирусных средств и методов их применения. Антивирусные средства применяются для решения следующих задач:

- обнаружение вирусов в КС;
- блокирование работы программ-вирусов;
- устранение последствий воздействия вирусов.

Обнаружение вирусов желательно осуществлять на стадии их внедрения или, по крайней мере, до начала осуществления деструктивных действий вирусов. Не существует антивирусных средств, гарантирующих обнаружение всех возможных вирусов.

При обнаружении вируса необходимо сразу же прекратить работу программы-вируса, чтобы минимизировать ущерб от его воздействия на систему.

Устранение последствий воздействия вирусов ведется в двух направлениях:

- удаление вирусов;
- восстановление (при необходимости) файлов, областей памяти.

Восстановление системы зависит от типа вируса, а также от момента времени обнаружения вируса по отношению к началу деструктивных действий. Восстановление информации без использования дублирующей информации может быть невыполнимым, если вирусы при внедрении не сохраняют информацию, на место которой они помещаются в память, а также, если деструктивные действия уже начались, и они предусматривают изменения информации.

Для борьбы с вирусами используются программные и аппаратно-программные средства, которые применяются в определенной последовательности и комбинации, образуя методы борьбы с вирусами, подразделяемые на:

- методы обнаружения вирусов;
- методы удаления вирусов.

2.1. Методы обнаружения вирусов

- ***сканирование*** осуществляется программой-сканером, которая просматривает файлы в поисках опознавательной части вируса – сигнатуры. Программа фиксирует наличие уже известных вирусов, за исключением полиморфных вирусов, которые применяют шифрование тела вируса, изменяя при этом каждый раз и сигнатуру. Программы-сканеры могут хранить не сигнатуры известных вирусов, а их контрольные суммы. Программы-сканеры часто могут удалять обнаруженные вирусы. Такие программы называют полифагами. Пример – Aidstest Дмитрия Лозинского;

- ***обнаружение изменений*** (базируется на использовании программ-ревизоров, которые определяют и запоминают характеристики всех областей на дисках, в которых обычно размещаются вирусы). При периодическом выполнении программ-ревизоров сравниваются хранящиеся характеристики и характеристики, получаемые при контроле областей дисков, по результатам которых программа выдает сообщение о предположительном наличии вирусов. Недостатки метода – с помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему уже зараженными; вирусы будут обнаружены только после размножения в системе;

- ***эвристический анализ*** позволяет определить неизвестные вирусы, но не требует предварительного сбора, обработки и хранения информации о файловой системе. Сущность метода – проверка возможных сред обитания вирусов и выявление в них команд (групп команд), характерных для вирусов (команды создания резидентных модулей в ОП, команды прямого обращения к дискам, минуя ОС);

- ***использование резидентных сторожей*** основан на применении программ, которые постоянно находятся в ОП ЭВМ и отслеживают все действия остальных программ: при выполнении каких-либо подозрительных действий (обращение для записи в загрузочные сектора, помещение в ОП резидентных модулей, попытки перехвата прерываний и т.п.) резидентный сторож выдает сообщение пользователю. Недостаток – значительный процент ложных тревог, что мешает работе и вызывает раздражение пользователя;

- ***вакцинирование программ*** (создание специального модуля для контроля ее целостности). В качестве характеристики целостности файла обычно используется контрольная сумма. При заражении вакцинированного файла, модуль контроля обнаруживает изменение контрольной суммы и сообщает об этом пользователю. Метод позволяет обнаруживать все вирусы, в т.ч. и незнакомые, за исключением «стелс»-вирусов);

- ***аппаратно-программная защита от вирусов*** (самый надежный метод защиты). В настоящее время используются специальные контроллеры и их программное обеспечение. Контроллер устанавливается в разъем расширения и имеет доступ к общей шине, что позволяет ему контролировать все обращения к дисковой системе. В программном обеспечении контроллера запоминаются области на дисках, изменение которых в обычных режимах работы не допускается. Можно устанавливать защиту на изменение главной загрузочной записи, загрузочных секторов, файлов конфигурации, исполняемых файлов и др.

2.2. Методы удаления последствий заражения вирусами

Существует два метода удаления последствий воздействия вирусов антивирусными программами:
первый – предполагает восстановление системы после воздействия известных вирусов (разработчики программы-фага, удаляющей вирус, должен знать структуру вируса и его характеристики размещения в среде обитания);
второй – позволяет восстанавливать файлы и загрузочные сектора, зараженные неизвестными вирусами (для восстановления файлов программа восстановления должна заблаговременно создать и хранить информацию о файлах, полученную в условиях отсутствия вирусов). Имея информацию о незараженном файле и используя сведения об общих принципах работы вирусов, осуществляется восстановление файлов. Если вирус подверг файл необратимым изменениям, то восстановление возможно только

с использованием резервной копии или с дистрибутива. При их отсутствии существует только один выход – уничтожить файл и восстановить его вручную.

2.3. Антивирусная утилита AVZ

Антивирусная утилита AVZ предназначена для обнаружения и удаления:

SpyWare и AdWare модулей - это основное назначение утилиты;

- Dialer (Trojan.Dialer);
- Троянских программ;
- BackDoor модулей;
- Сетевых и почтовых червей;
- TrojanSpy, TrojanDownloader, TrojanDropper.

Утилита является прямым аналогом программ TrojanHunter и LavaSoft Ad-aware 6. Первичной задачей программы является удаление SpyWare и троянских программ. Интерфейс программы представлен на рисунке 1.

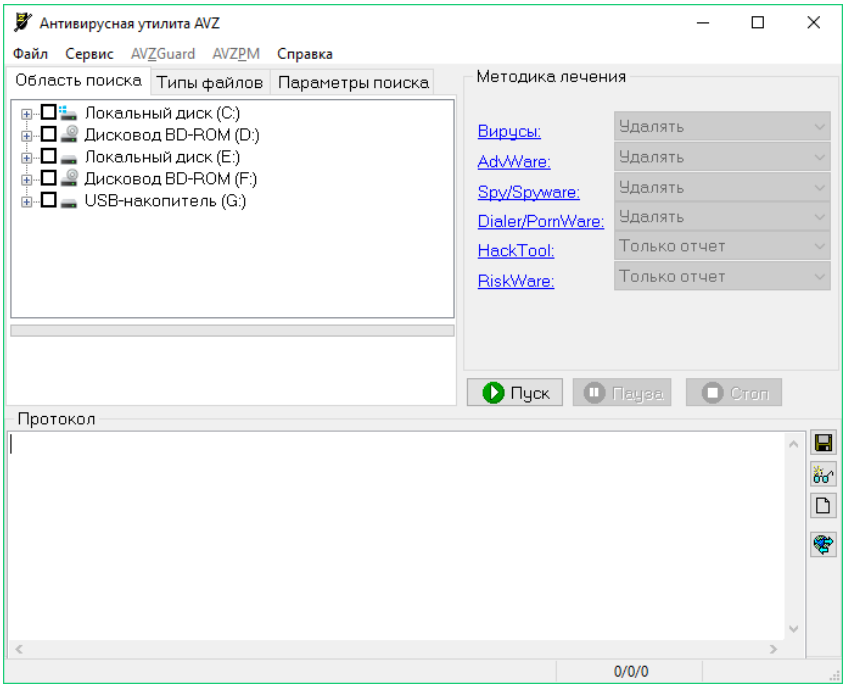

Рис. 1. – Главный экран AVZ

Запуск утилиты должен производиться от имени администратора.

Особенностями утилиты AVZ (помимо типового сигнатурного сканера) является:

- **Микропрограммы эвристической проверки системы**. Микропрограммы проводят поиск известных SpyWare и вирусов по косвенным признакам - на основании анализа реестра, файлов на диске и в памяти.
- **Обновляемая база безопасных файлов**. В нее входят цифровые подписи десятков тысяч системных файлов и файлов известных безопасных процессов. База подключена ко всем системам AVZ и работает по принципу "свой/чужой" - безопасные файлы не вносятся в карантин, для них заблокировано удаление и вывод предупреждений, база используется антируткитом, системой поиска файлов, различными анализаторами. В частности, встроенный диспетчер процессов выделяет безопасные процессы и сервисы цветом, поиск файлов на диске может исключать из

поиска известные файлы (что очень полезно при поиске на диске троянских программ);

- **Встроенная система обнаружения Rootkit**. Поиск RootKit идет *без применения сигнатур* на основании исследования базовых системных библиотек на предмет перехвата их функций. AVZ может не только обнаруживать RootKit, но и производить корректную блокировку работы UserMode RootKit для своего процесса и KernelMode RootKit на уровне системы. Противодействие RootKit распространяется на все сервисные функции AVZ, в результате сканер AVZ может обнаруживать маскируемые процессы, система поиска в реестре "видит" маскируемые ключи и т.п. Антируткит снабжен анализатором, который проводит обнаружение процессов и сервисов, маскируемых RootKit. Одной из главных на мой взгляд особенностей системы противодействия RootKit является ее работоспособность в Win9X (распространеннное мнение об отсуствии RootKit, работающих на платформе Win9X глубоко ошибочно - известны сотни троянских программ, перехватывающих API функции для маскировки своего присутствия, для искажения работы API функций или слежения за их использованием). Другой особенностью является универсальная система обнаружения и блокирования KernelMode RootKit, работоспособная под Windows NT, Windows 2000 pro/server, XP, XP SP1, XP SP2, Windows 2003 Server, Windows 2003 Server SP1
- **Детектор клавиатурных шпионов (Keylogger) и троянских DLL**. Поиск Keylogger и троянских DLL ведется на основании анализа системы *без применения базы сигнатур*, что позволяет достаточно уверенно детектировать заранее неизвестные троянские DLL и Keylogger;
- **Нейроанализатор**. Помимо сигнатурного анализатора AVZ содержит нейроэмулятор, который позволяет производить исследование подозрительных файлов при помощи нейросети. В настоящее время нейросеть применяется в детекторе кейлоггеров.
- **Встроенный анализатор Winsock SPI/LSP настроек**. Позволяет проанализировать настройки, диагностировать возможные ошибки в настройке и произвести *автоматическое* лечение. Возможность автоматической диагностики и лечения полезна для начинающих пользователей (в утилитах типа LSPFix автоматическое лечение отсутствует). Для исследования SPI/LSP вручную в программе имеется специальный менеджер настроек LSP/SPI. На работу анализатора Winsock SPI/LSP распространяется действие антируткита;
- **Встроенный диспетчер процессов, сервисов и драйверов**. Предназначен для изучения запущенных процессов и загруженных библиотек, запущенных сервисов и драйверов. На работу диспетчера процессов распространяется действие антируткита (как следствие - он "видит" маскируемые руткитом процессы). Диспетчер процессов связан с базой безопасных файлов AVZ, опознанные безопасные и системные файлы выделяются цветом;
- **Встроенная утилита для поиска файлов на диске**. Позволяет искать файл по различным критериям, возможности системы поиска превосходят возможности системного поиска. На работу системы поиска распространяется действие антируткита (как следствие - поиск "видит" маскируемые руткитом файлы и может удалить их), фильтр позволяет исключать из результатов поиска файлы, опознанные AVZ как безопасные. Результаты поиска доступны в виде текстового протокола и в виде таблицы, в которой можно пометить группу файлов для последующего удаления или помещения в карантин
- **Встроенная утилита для поиска данных в реестре**. Позволяет искать ключи и параметры по заданному образцу, результаты поиска доступны в виде текстового протокола и в виде таблицы, в которой можно отметить несколько ключей для их экспорта или удаления. На работу системы поиска распространяется действие

антируткита (как следствие - поиск "видит" маскируемые руткитом ключи реестра и может удалить их)

- **Встроенный анализатор открытых портов TCP/UDP**. На него распространяется действие антируткита, в Windows XP для каждого порта отображается использующий порт процесс. Анализатор опирается на обновляемую базу портов известных троянских/Backdoor программ и известных системных сервисов. Поиск портов троянских программ включен в основной алгоритм проверки системы - при обнаружении подозрительных портов в протокол выводятся предупреждения с указанием, каким троянских программам свойственно использование данного порта
- **Встроенный анализатор общих ресурсов**, сетевых сеансов и открытых по сети файлов. Работает в Win9X и в NT/W2K/XP.
- **Встроенный анализатор Downloaded Program Files (DPF)** - отображает элементы DPF, подключен ко всем системам AVZ.
- **Микропрограммы восстановления системы**. Микропрограммы проводят восстановления настроек Internet Explorer, параметров запуска программ и иные системные параметры, повреждаемые вредоносными программами. Восстановление запускается вручную, восстанавливаемые параметры указываются пользователем.
- **Эвристическое удаление файлов**. Суть его состоит в том, что если в ходе лечения удалялись вредоносные файлы и включена эта опция, то производится автоматическое исследование системы, охватывающее классы, BHO, расширения IE и Explorer, все доступные AVZ виды автозапуска, Winlogon, SPI/LSP и т.п. Все найденные ссылки на удаленный файл автоматически вычищаются с занесением в протокол информации о том, что конкретно и где было вычищено. Для этой чистки активно применяется движок микропрограмм лечения системы;
- **Проверка архивов.** Начиная с версии 3.60 AVZ поддерживает проверку архивов и составных файлов. На настоящий момент проверяются архивы формата ZIP, RAR, CAB, GZIP, TAR; письма электронной почты и MHT файлы; CHM архивы
- **Проверка и лечение потоков NTFS.** Проверка NTFS потоков включена в AVZ начиная с версии 3.75
- **Скрипты управления.** Позволяют администратору написать скрипт, выполняющий на ПК пользователя набор заданных операций. Скрипты позволяют применять AVZ в корпоративной сети, включая его запуск в ходе загрузки системы.
- **Анализатор процессов.** Анализатор использует нейросети и микропрограммы анализа, он включается при включении расширенного анализа на максимальном уровне эвристики и предназначен для поиска подозрительных процессов в памяти.
- **Система AVZGuard.** Предназначена для борьбы с трудноудалимыми вредоносными программами, может кроме AVZ защищать указанные пользователем приложения, например, другие антишпионские и антивирусные программы.
- **Система прямого доступа к диску** для работы с заблокированными файлами. Работает на FAT16/FAT32/NTFS, поддерживается на всех операционных системах линейки NT, позволяет сканеру анализировать заблокированные файлы и помещать их в карантин.
- **Драйвер мониторинга процессов и драйверов AVZPM**. Предназначен для отслеживания запуска и остановки процессов и загрузки/выгрузки драйверов для поиска маскирующихся драйверов и обнаружения искажений в описывающих процессы и драйверы структурах, создаваемых DKOM руткитами.
- **Драйвер Boot Cleaner**. Предназначен для выполнения чистки системы (удаление файлов, драйверов и служб, ключей реестра) из KernelMode. Операция чистки может выполняться как в процессе перезагрузки компьютера, так и в ходе лечения.

3. Задание для выполнения работы

Изучить категории вредоносных программ и изучить работу с антивирусной утилитой AVZ.

4. Методика выполнения работы

4.1. Изучите основные теоретические сведения.

4.2. Заполнить таблицу с описанием вирусов*

Категории вредоносных программ	**Наименование и описание вируса**	**Видимые проявления**
Adware и SpyWare		
Backdoor		
Hoax		
Trojan		
Trojan-Clicker		
Trojan-Downloader		
Trojan-Spy		
Trojan-PSW		
Net-Worm		
Worm		
Trojan-Dropper		
Trojan-Proxy		
Email-Worm		
FraudTool		

Trojan-Ransom		

**** данные для таблицы можно найти на официальном сайте AVZ***

4.3. Запустить утилиту AVZ

4.4. Включить AVZGuard

4.5. Выполнить восстановление настроек системы: без «Полного пересоздания настроек SPI».

4.6. Выполнить резервное копирование с параметрами: настройки проводника, настройки рабочего стола и настройки Windows Firewall.

4.7. Используя «Мастер поиска и устранения проблем» произвести поиск проблем средней тяжести и исправить их.

4.8. Используя диспетчер процессов определить используемые модули для процесса «smss.exe».

4.9. Используя менеджер файла Hosts убедиться в отсутствии лишних записей.

4.10. Узнать какие порты TCP/UDP открыты.

4.11. Провести поиск на наличие уязвимостей и вирусов. Выставив следующие настройки:

а) методика лечения: удалять все
б) область поиска: все диски
в) эвристический анализ: средний уровень
г) Anti-RootKit: детектировать перехватчики
д) keylogger – включен
е) поиск портов TCP/UDP троянских программ – включен
ж) копировать подозрительные файлы в карантин
з) тип файлов: все файлы

4.12. Сохранить профиль настроек для дальнейшего использования.

4.13. Завершить работу с утилитой AVZ.

5. Оформление отчета

Отчет по выполненной работе представляется в печатном или рукописном виде и должен включать:

- титульный лист;
- теоретические сведения;
- описание работы утилиты AVZ;
- вывод по работе;
- ответы на контрольные вопросы.

Контрольные вопросы

1. Какие существуют методы обнаружения вирусов?
2. Какие из методов позволяют определить неизвестные вирусы?
3. Какие существуют методы удаления последствий заражения вирусами?
4. Для чего предназначена антивирусная утилита AVZ?
5. Что такое руткит?