Министерство образования XXX

Государственное бюджетное профессиональное образовательное учреждение

XXX «Колледж «XXX»

09.02.07

ОТЧЕТ

По лабораторным работам

МДК 04.02 Обеспечение качества функционирования компьютерных систем

ККОО.ПМ.XXX.000

Студент XXX

Преподаватель XXX

Дата защиты_____ Оценка_____

2022

Лабораторная работа №5.3

«Обнаружение вируса и устранение последствий его влияния»

Цель работы: «изучение методов обнаружения вирусов и методов удаления последствий заражения вирусами с использованием антивирусной утилиты AVZ»

Краткие 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.

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.).

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).

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.

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 отсутствии 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.

Порядок выполнения лабораторной работы:

1. Изучить теоретический материал.
2. Выполнить предлагаемые задания.
3. Ответить на контрольные вопросы и предоставить отчет.

Задания для выполнения лабораторной работы:

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

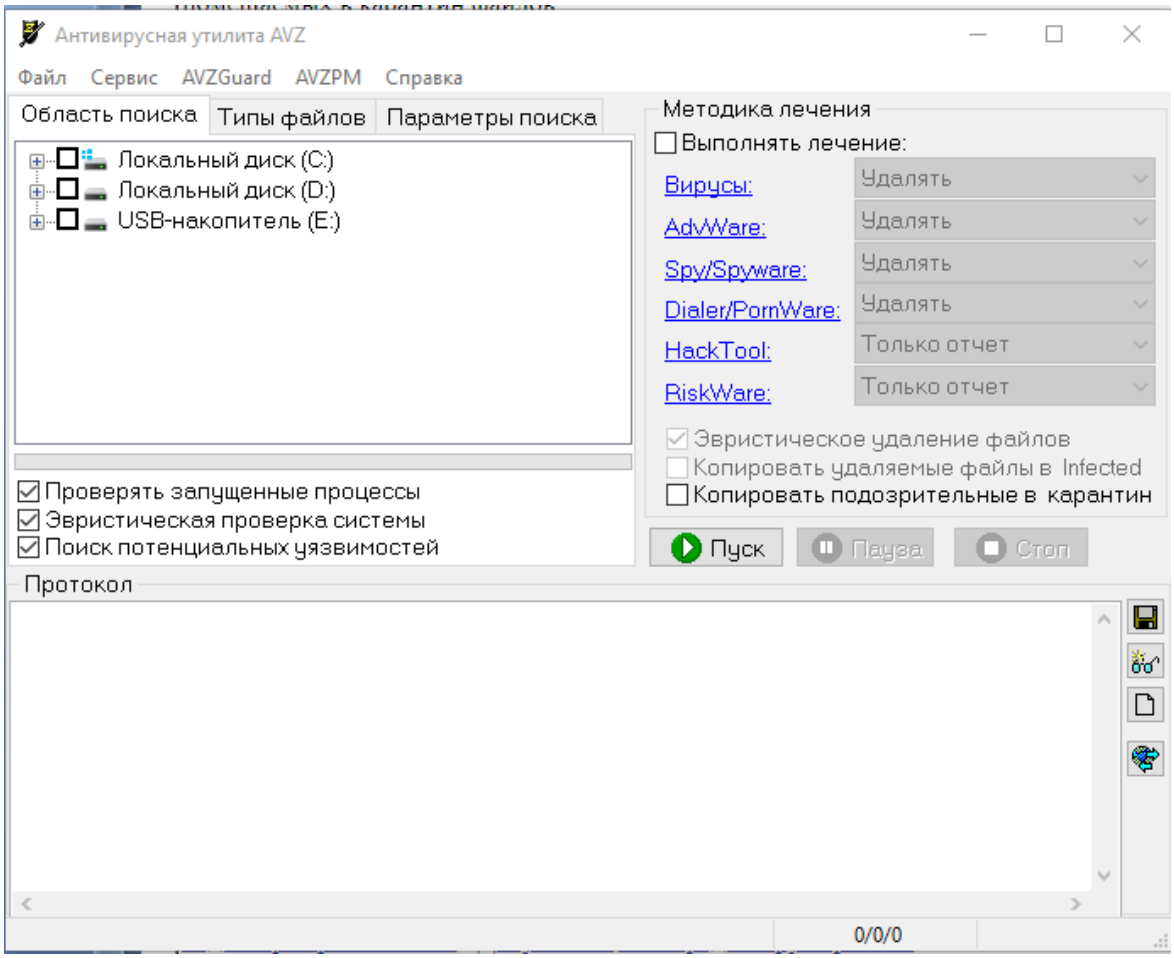

Рисунок 1 Главный экран

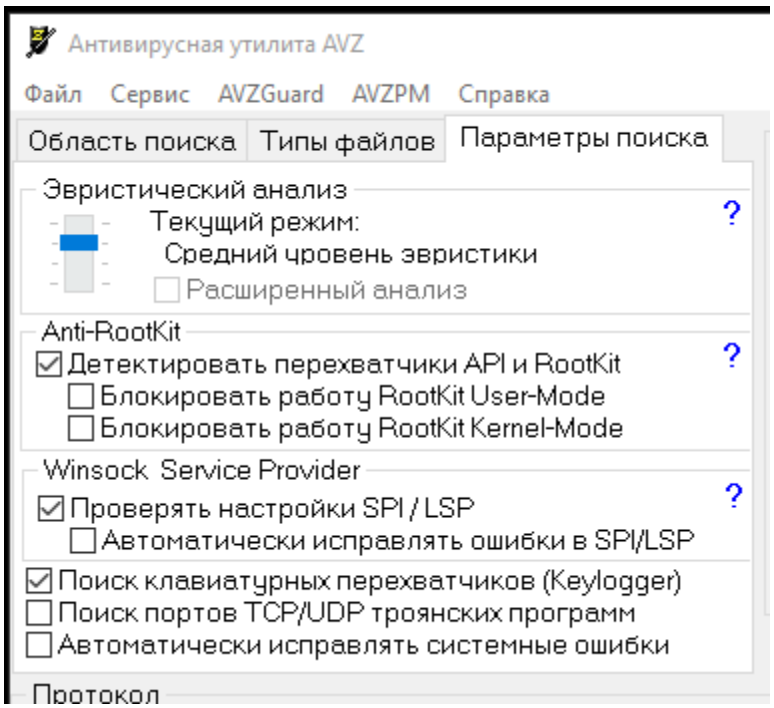

Рисунок 2 Вкладка «Параметры поиска»

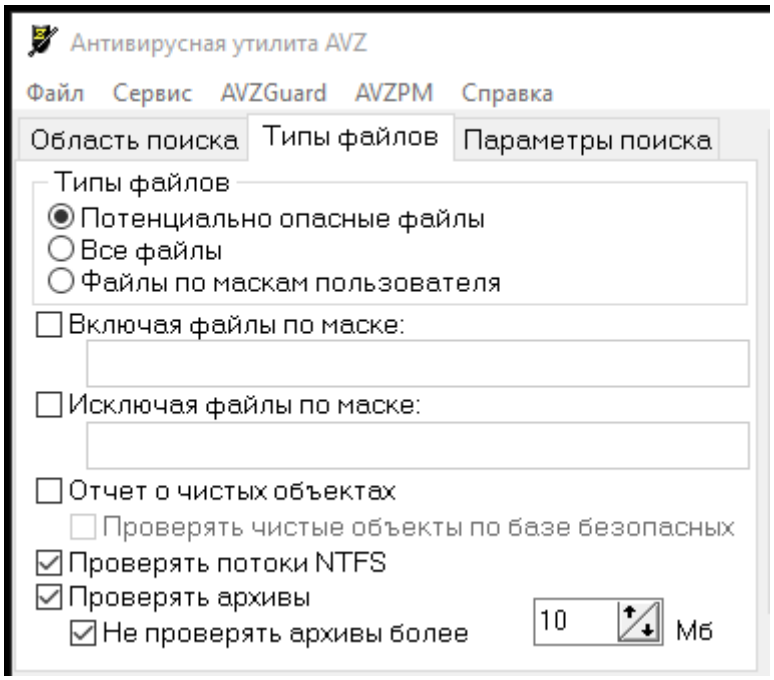

Рисунок 3 Вкладка «Типы файлов»

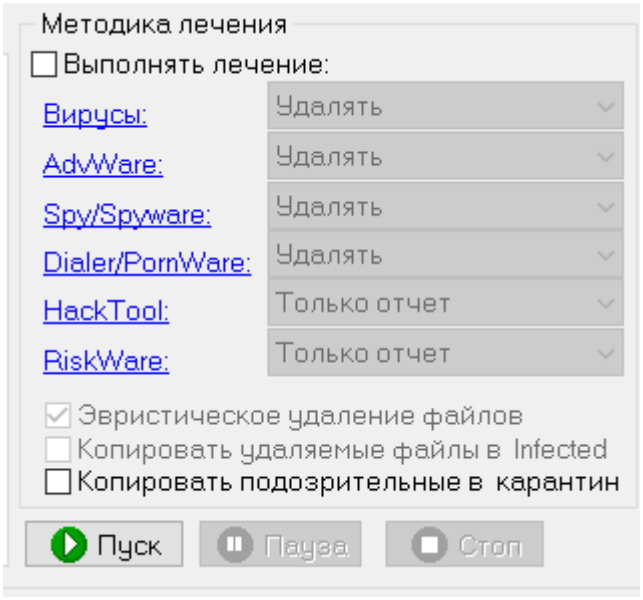

Рисунок 4 Методики лечения и кнопка «Пуск»

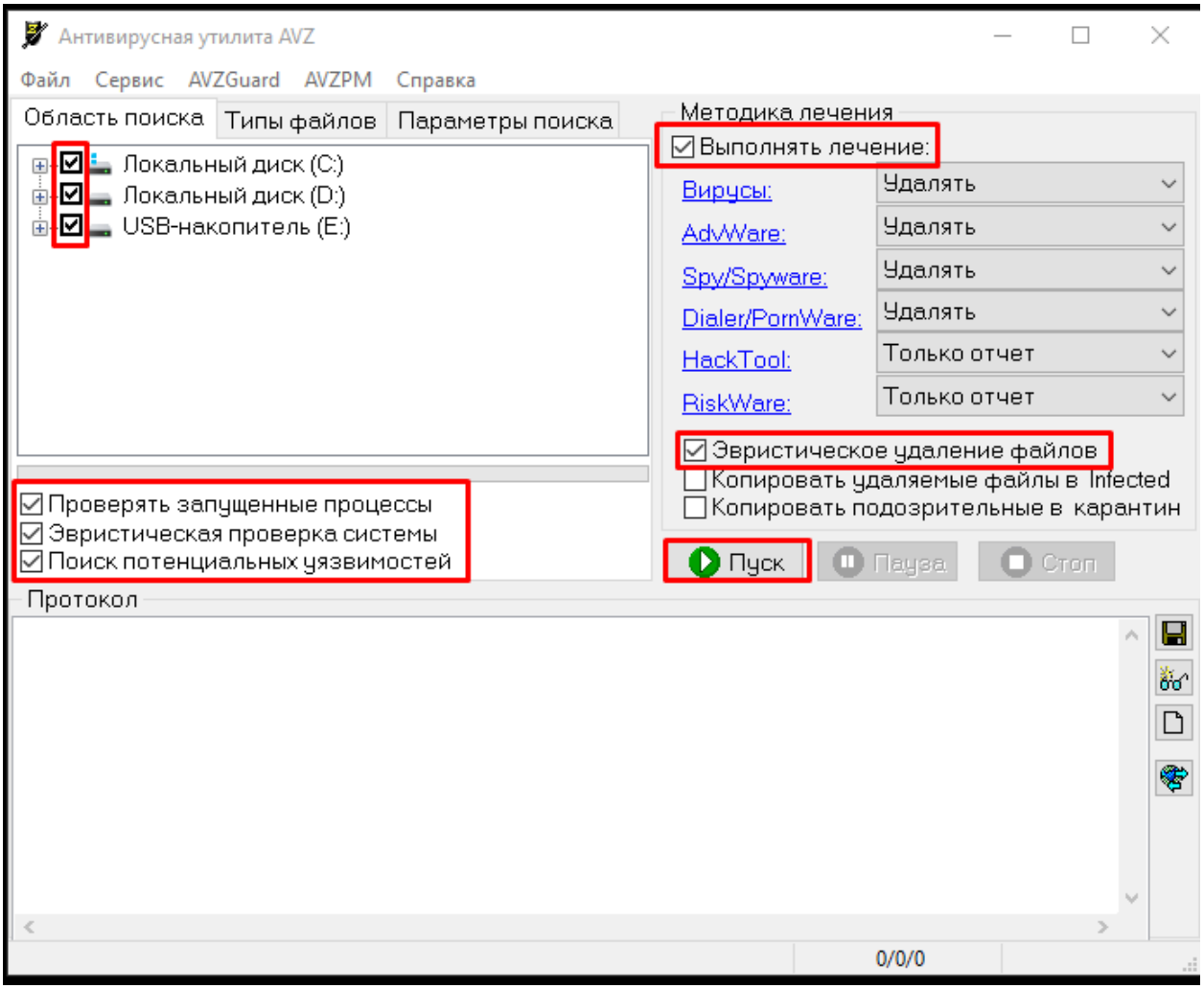

Рисунок 5 Необходимые настройки для выполнения сканирования

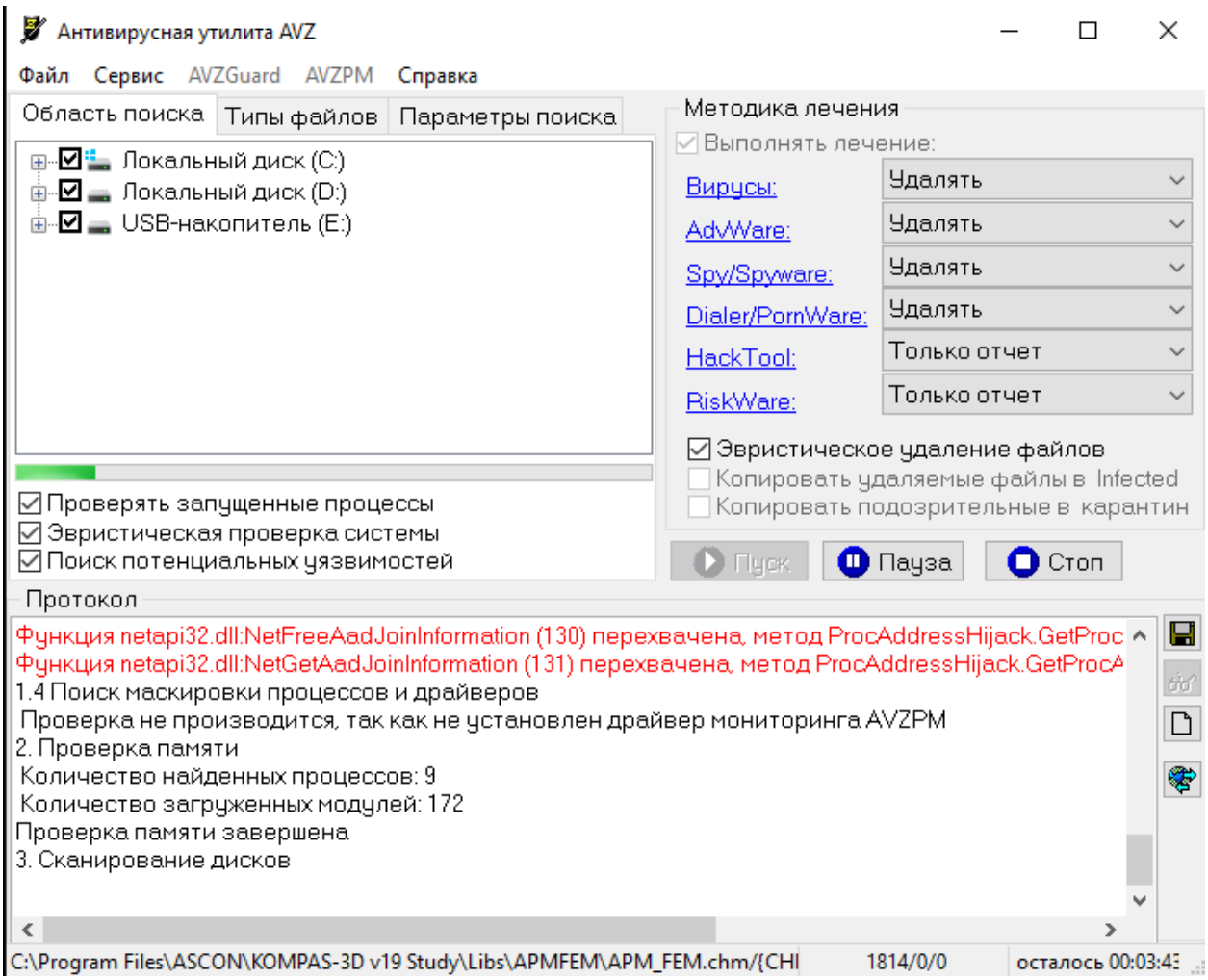

Рисунок 6 Процесс сканирования

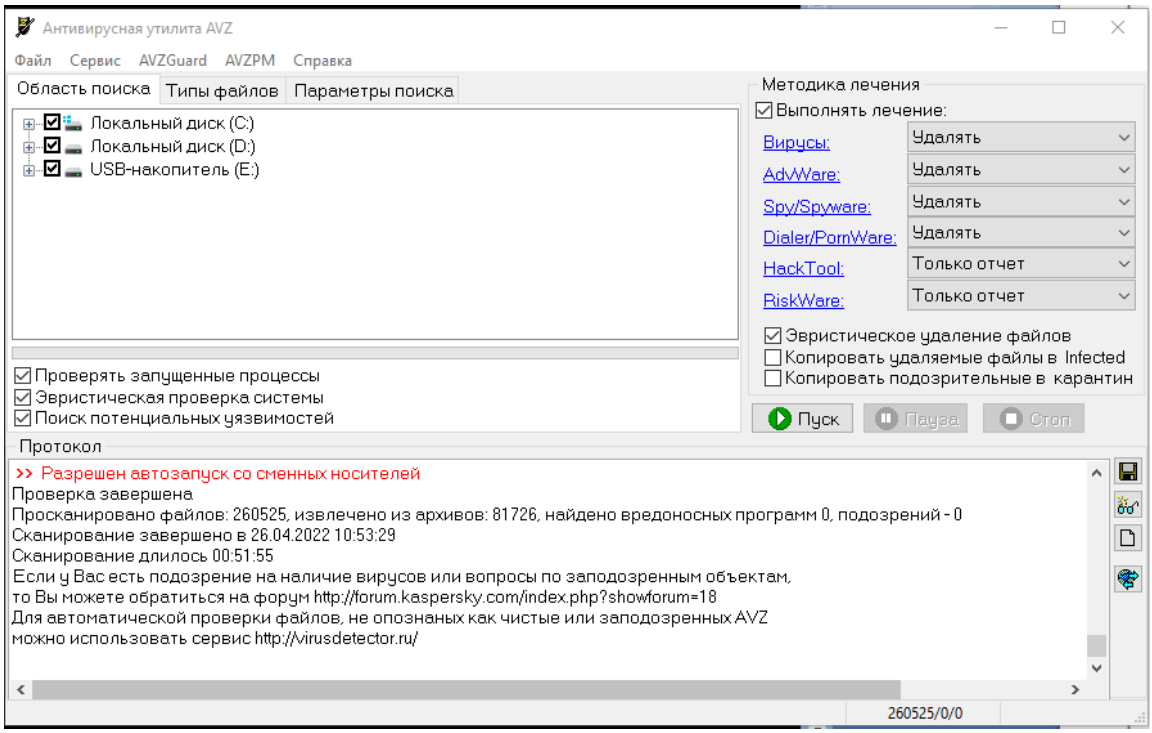

Рисунок 7 Завершенное сканирование

Заполнить таблицу с описанием вирусов

Категории вредоносных программ	Наименование и описание вируса	Видимые проявления
Adware и SpyWare	SpyWare – вирусы – шпионы, собирают информацию о действиях и поведении пользователя. В основном их интересует такая информация, как: адреса, пароли, данные кредитных карт). Adware - рекламные вирусы, без ведома пользователей встраиваются в различное программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама	Adware - рекламные вирусы, без ведома пользователей встраиваются в различное программное обеспечение с целью демонстрации рекламных объявлений. SpyWare в основном можно заметить в Диспетчере Задач, когда вы нажали на загруженный из интернета .exe или файл другого расширения, так как SpyWare обычно работает только первые несколько минут, после чего отправляет всю собранную информацию злоумышленнику и затем самоуничтожается.

	располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе.	
Backdoor	Дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удалённому управлению операционной системой и компьютером в целом	Backdoor является очень скрытым вирусом(уязвимостью). Чтобы заметить какую-то активность, желательно воспользоваться программой Wireshark в случае, если вы используете программу, связанную с работой по сети. В Wireshark вы можете проанализировать сетевую активность и увидеть лишние подключение или исходящий трафик.
Hoax	сообщение, предупреждающее получателей о несуществующем	Заметить данный вирус достаточно просто. Достаточно после установки очередной

	компьютерном вирусе или иной угрозе.	нужной вам программы посмотреть на ее действия в вашей операционной системе. Если вы часто видите какие-то всплывающие окна, которые являются приманкой для вас, можете уже начинать думать, что программа, которую вы установили, является недобросовестной и возможно имеет какие-то другие встроенные скрытые функции.
Trojan	Разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно.	Заметить троянца не очень просто без установленного антивируса. Обычно троянцы могут изменять каким-либо образом файлы, проявлять повышенную сетевую активность.
Trojan-Clicker	Кликфрод — один из видов сетевого мошенничества,	Заметить троянца не очень просто без установленного антивируса. Заметить

	представляющий собой обманные клики на рекламную ссылку лицом, не заинтересованным в рекламном объявлении. Кликфрод может осуществляться как раз с помощью автоматизированного вируса, в случае которого злоумышленнику будут приходить деньги за счет кликфрода с вашего ПК.	именно троянца-кликфродера можно с помощью программы Wireshark, в ней можно будет увидеть конкретные запросы на разные сайты, содержащие рекламу.
Trojan-Downloader	Вредоносная программа, предназначенная для несанкционированной пользователем загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки троянцев или рекламных систем.	Заметить троянца не очень просто без установленного антивируса. Заметить троянца-загрузчика будет довольно сложно, если он самоуничтожается после своей работы. Хотя есть и те, которые не самоуничтожаются, но они уже являются не просто загрузчиками, а чем-то наподобие ботнета.
Trojan-Spy	Программы категории	Заметить данного троянца

	Trojan-SPY предназначены для явного шпионажа за пользователем. Это в первую очередь клавиатурные шпионы, всевозможные системы слежения за активностью пользователя. Интересной особенностью многих программ данной категории является то, что они зачастую вполне легально распространяются и продаются, снабжены подробной документаций и инсталлятором. Однако решаемые ими задачи (скрытный сбор информации, скрытная отправка собранной информации в соответствии с настройками не оставляет сомнений в вредоносности данных	довольно легко с помощью программы Wireshark, так как данный троянец постоянно отправляют информацию на сервер злоумышленника.

	программ).	
Trojan-PSW	Троянские программы категории Trojan-PSW представляют большую опасность для пользователя, т.к. их основное назначение состоит в поиске на пораженном компьютере паролей пользователя для их последующей отправки злоумышленникам.	При запуске зараженного файла, если там содержится данный троянец, заметить его будет не очень просто без установленного антивируса. Данный троянец соберет всю информацию с браузеров и прочих приложений в течение 30-40 секунд, после чего отправит эту информацию на сервер злоумышленника и самоуничтожится. Чтобы избежать данной проблемы, необходимо обязательно иметь антивирус, либо вместе с запускаемым неизвестным приложением держать открытой программы Wireshark и смотреть на сетевую активность данной программы. Если вы заметили что-то подозрительное, чтобы обезвредить данную программу, достаточно просто отключить интернет

		от своего ПК.
Net-Worm	Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению в компьютерных сетях. Отличительной особенностью данного типа червей является отсутствие необходимости в пользователе как в звене в цепочке распространения (т.е., непосредственно для активации вредоносной программы).	Данный вирус достаточно просто обнаружить с помощью антивируса или с инструментов анализа сети, например Wireshark, так как он проявляет очень высокую сетевую активность. Если не обнаружить его вовремя, он может очень быстро заразить множество компьютеров в сети.
Worm	Червь – программа, которая делает копии самой себя. Ее вред заключается в захламлении компьютера, из-за чего он начинает работать медленнее.	Данный вирус достаточно просто обнаружить с помощью антивируса. В случае отсутствия антивируса на вашем компьютере, необходимо посмотреть процессы в диспетчере задач на наличие сторонних задач.

Trojan-Dropper	Троянец-дроппер (trojan dropper), или просто дроппер (Dropper) — вредоносное программное обеспечение, предназначенное для доставки на компьютер или смартфон жертвы другого вредоносного ПО.	Заметить троянца не очень просто без установленного антивируса. Заметить троянца-дроппера будет довольно сложно, если он самоуничтожается после своей работы.
Trojan-Proxy	Вредоносная программа, предназначенная для осуществления злоумышленником несанкционированного пользователем анонимного доступа к различным интернет-ресурсам через компьютер-жертву. Данный тип вредоносных программ обычно используется при рассылке спама через заражённые компьютеры	Заметить данного троянца очень легко при помощи Wireshark. Через ваш компьютер при анализе сети будет видно очень много различных соединений как из других стран, так и из России. Также будет видно очень много постоянных соединений с различными сайтами.

Email-Worm	Вредоносная программа, обладающая способностью к несанкционированному пользователем саморазмножению по каналам электронной почты. В процессе размножения червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе (например, URL на зараженный файл, расположенный на взломанном или хакерском веб-сайте).	Заметить данного червя достаточно просто, так как достаточно проверять отправленные вами почтовые сообщение и регулярно делать проверку своего компьютера антивирусом.
FraudTool	Программы, которые выдают себя за другие программы, хотя таковыми не являются. В качестве примера таких программ можно привести псевдоантивирусы, которые выводят	Часто предлагают пользователю перечислить финансовые средства на определенные счета для оплаты «услуг».

	сообщения об «обнаружении» вредоносных программ, но на самом деле ничего не находят и не лечат.	
Trojan-Ransom	Программы категории Trojan-Ransom предназначены для вымогательства. Приемов реализации множество, однако алгоритм в основном сводится к двум пунктам: 1. Создание проблемы или имитация ее наличия - блокировка работы компьютера, создание каких-либо помех в работе браузера или иных прикладных программ, имитация наличия на компьютере вирусов, шифровка файлов пользователя; 2. Предложение решить данную проблему за	Если вы обнаружили данный вирус, считайте ваш компьютер уже в беде, так как если вы запустили софт, содержащий данный вирус, вы можете сразу заметить, как ваши файлы начнут менять расширение и на рабочем столе могут появляться файлы .txt с посланием для вас. Возможна смена обоев рабочего стола на предупреждение о заражении данной машины с посланием от злоумышленников. Если вы все это заметили, можете переустанавливать полностью операционную систему, если данный вирус не вшивается в BIOS вашей системы. Никогда не оплачивайте дешифрование

	определенную сумму денег - как правило, предлагается или совершить перевод указанной суммы, или послать SMS, или купить карты экспресс-оплаты и прислать их PIN коды. Важно отметить, что оплата не гарантирует решение проблемы	компьютера злоумышленникам, так как в 99% случаях это обман. Конечно, маловероятно что вы окажетесь жертвой такого вируса, так как в основном злоумышленники атакуют предприятия данным вирусом, а не обычных пользователей.

Контрольные вопросы:

1. Какие существуют методы обнаружения вирусов?

- Сканирование (осуществляется программой - сканером, которая просматривает файлы в поисках опознавательной части вируса – сигнатуры).
- Обнаружение изменений (базируется на использовании программ – ревизоров, которые определяют и запоминают характеристики всех областей на дисках, в которых обычно размещаются вирусы).
- Эвристический анализ (суть этого метода заключается в проверке возможных сред обитания вирусов и выявлении в них команд, характерных для вирусов).
- Использование резидентных сторожей (метод основан на применении программ, которые постоянно находятся в ОП ЭВМ и отслеживают все действия остальных программ).
- Вакцинирование программ (создание специального модуля для контроля ее целостности.).

- Аппаратно – программная защита от вирусов (считается самым надежным методом защиты, заключается в использовании специальных контроллеров и их ПО).

2. Какие из методов позволяют определить неизвестные вирусы?

Неизвестные вирусы позволяет определить эвристический анализ.

3. Какие существуют методы удаления последствий заражения вирусами?

- Первый метод предполагает восстановление системы после воздействия известных вирусов (разработчики программы-фага, удаляющей вирус, должен знать структуру вируса и его характеристики размещения в среде обитания);
- Второй метод 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).

4. Для чего предназначена антивирусная утилита AVZ?

Антивирусная утилита AVZ предназначена для обнаружения и удаления:

- SpyWare и AdWare модулей - 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.

5. Что такое руткит?

Руткит - программа, которая скрывает от антивирусов собственные вредоносные действия, либо маскирует работу другого вредоносного ПО — например, трояна.