**Практическая работа №18. Часть 2. Диагностика Антивирусного пакета**

***Сценарий****. Завершающий этап установки любой программы - это проверка корректности выполнения основных ее функций. Для антивирусных приложений основу функционала составляет способность находить и обезвреживать вредоносные программы.*

*Естественно, встает вопрос как проверить действительно ли**программа может это делать - ведь известно, что новые вирусы появляются каждый день, причем десятками, а иногда и сотнями. Не каждому пользователю под силу регулярно отслеживать хотя бы их часть. Этим занимаются антивирусные компании. Их филиалы, разбросанные по всему миру, непрерывно следят за вирусной активностью в**Интернет, перехватывают и анализируют все подозрительные файлы. На основе полученных данных формируются вирусные сигнатуры, которые рядовой**пользователь получает во время обновления своих антивирусных баз. Таким образом, проверить**надежность антивирусной защиты от всех уже существующих вирусов и тех, которые только завтра или через год будут созданы, нереально. К тому же, использовать настоящие вирусы только для предварительного тестирования программы нельзя. Нельзя исключать**вероятность, что**программа установки где-то дала сбой и следовательно защита не установлена. Тогда во время проверки может произойти заражение вирусом, на котором производится тестирование, что недопустимо.*

*Но несмотря на все эти проблемы, метод диагностики антивирусных программ все же существует. Для этого используется специальный**файл, " The Anti-**Virus or**Anti-Malware test file ", созданный Европейским институтом компьютерных антивирусных исследований (European Institute for**Computer**Antivirus Research).*

*В задании 1 этой части предлагается познакомиться с тестовым вирусом, в заданиях 2, 3 и 4 - протестировать работу установленного у вас антивирусного пакета (какой у вас установлен – не знаю, все действия выполняются под Антивирус Касперского, если нет никакого - см. часть 1 этой работы), параллельно изучив структуру резервного хранилища и карантина.*

**Задание 1. Тестовый вирус**

*Тестовый**вирус, разработанный Европейским институтом компьютерных антивирусных исследований, называется EICAR - по аббревиатуре полного названия института (European Institute for**Computer**Antivirus Research).*

*EICAR представляет собой небольшой 68-байтный**файл. Его расширение можно варьировать в зависимости от сценария тестирования. Если добавить .com, то**запуск получившегося файла eicar.com на незащищенном компьютере вызовет только 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 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.*

*Если открыть EICAR в каком-либо текстовом редакторе, например****Блокнот****(****Notepad****), то обнаружится, что он состоит из 68 символов:*

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

*Следовательно, тестовый**вирус в любой момент можно создать самостоятельно. Для этого нужно только открыть любой**текстовый редактор, набрать в нем эту строку и сохранить получившийся**файл в формате текстового файла (обычный текст).*

*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.*

*Поэтому для тестирования антивирусных продуктов****Лаборатория Касперского****предлагает использовать модифицированный тестовый**вирус, а именно:*

|  |  |  |
| --- | --- | --- |
| **№** | **Файл** | **Описание** |
| 1 | *CURE*-EICAR | Обнаружив такой файл, антивирус должен его "вылечить", сократив его размер до 4 байт (символы "*CURE*" ) |
| 2 | DELE-EICAR | Этот файл **Антивирус Касперского** определяет как неизлечимый вирус или троянскую программу и удаляет. Следовательно, по результатам проверки DELE-EICAR должен быть обнаружен только в резервном хранилище |
| 3 | CORR-EICAR | Предназначен для диагностики работы **Антивируса Касперского** в случае обнаружения файла с поврежденной структурой, вследствие чего проверить его на наличие вирусов невозможно. Такой файл признается условно чистым |
| 4 | ERRO-EICAR | При сканировании такого файла **Антивирус Касперского** должен вести себя так, как будто произошла ошибка при анализе его содержимого (например, из-за нарушения целостности при проверке многотомного архива или при обрыве связи во время проверки по сети). ERRO-EICAR также признается условно чистым |
| 5 | SUSP-EICAR | Этот файл корректно работающий **Антивирус Касперского** признает подозрительным, а именно зараженным неизвестным вирусом. Следовательно, он должен быть помещен на карантин или удален (в зависимости от настроек, по умолчанию действие при обнаружении подозрительного объекта запрашивается у пользователя) |
| 6 | WARN-EICAR | WARN-EICAR также признается подозрительным, но не неизвестным вирусом, а модификацией известного. Это также приводит к предложению поместить его на карантин или удалить (в зависимости от настроек) |

*Создаются эти файлы по следующему принципу. 68-символьная строка с начала дополняется пятью символами, в зависимости от модификации - приставкой**CURE, DELE, CORR, ERRO, SUSP или WARN и дефисом. Например, содержимое**CURE-EICAR выглядит так:*

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

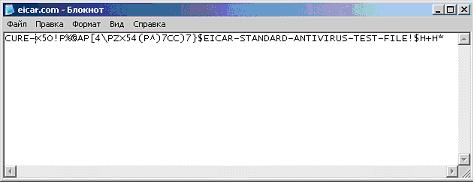
*В этом задании нужно создать тестовые вирусы EICAR,**CURE-EICAR и SUSP-EICAR.*

**Отчет. Заархивированная папка с вирусами.**

1. В этом задании нужно будет создать три файла с тестовыми вирусами: eicar.com, *cure*-eicar.com и susp-eicar.com. Для того, чтобы антивирус не заблокировал тестовые вирусы еще на подготовительном этапе, нужно временно отключить постоянную защиту.
2. Запустите текстовый редактор **Блокнот**
3. В открывшемся окне наберите строку

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

1. Сохраните получившийся файл в папку **Test** под именем eicar.com.
2. Вернитесь к окну **Блокнота**, нажав **Сохранить**
3. Модифицируйте EICAR, добавив к нему приставку "*CURE*-"



1. Сохраните получившийся файл под именем *cure*-eicar.com, воспользовавшись командой **Файл / Сохранить как…**
2. Аналогично создайте SUSP-EICAR, повторив пункты 6-7, но для приставки "SUSP-"
3. Закройте окно текстового редактора **Блокнот**
4. В результате этих действий в папке Test должно появиться три файла: eicar.com, *cure*-eicar.com и susp-eicar.com. Убедитесь в этом.
5. Проверьте размер каждого из файлов. Для этого по очереди наведите курсор мыши на каждый из файлов и ознакомьтесь с информацией, представленной во всплывающем окне.

Файл eicar.com должен иметь размер 68 байт, а *cure*-eicar.com и susp-eicar.com - по 73 байта

1. Убедитесь, что при запуске тестовый вирус выводит предупреждающее окно. Для этого запустите eicar.com, дважды щелкнув по нему курсором мыши
2. Поскольку EICAR представляет собой приложение MS DOS, то при его запуске откроется окно сеанса MS DOS, которое сразу же после выполнения программы закроется. Для того, чтобы увидеть сообщение про то, что EICAR - это тестовый вирус, нужно запустить его через командную строку.

Воспользуйтесь системным меню **Пуск / Программы/ Стандартные / Командная строка**

1. В открывшемся окне перейдите к каталогу **Test**.
2. Перейдя к нужному каталогу, запустите файл eicar.com, набрав команду

eicar.com

и нажав **Enter**

1. Ознакомьтесь с сообщением, которое вывел EICAR



1. Закройте окно командной строки, набрав exit и нажав клавишу **Enter**

**Задание 2. Тестирование с помощью EICAR**

*В этом задании нужно будет протестировать способность вашего антивируса обнаруживать вирусы на примере базового тестового вируса EICAR. Предлагается это сделать с помощью задачи поиска вирусов, запускаемой из контекстного**меню объектов.*

*В задании нужно будет при выключенной постоянной защите перейти к папке с тестовыми файлами , найти в ней eicar.com и проверить его на вирусы.*

***Антивирус*** *должен найти* *вирус в eicar.com и запросить дальнейшие действия у пользователя. Поскольку EICAR неизлечим,**функция лечения недоступна. Такие файлы всегда рекомендуется удалять, что и нужно будет выбрать в этом задании.*

*Дополнительно нужно проследить, что удаленные файлы не удаляются, а сначала перемещаются в резервное хранилище.*

**Отчет. Скрины выполнения следующих пунктов: №2, 3, 4, 6, 9.**

1. Перейдите к папке с тестовыми вирусами
2. Вызовите контекстное меню файла eicar.com и выберите пункт **Проверить на вирусы**
3. Как результат, почти одновременно должны появиться два окна. Сначала окно статистики выполнения задачи поиска вирусов
4. Поверх него в - окно с запросом действия.

*Обратите внимание, что окно запроса действия разделено на две области. Вверху - информация об обнаруженном вирусе: имя вируса с гиперссылкой на его описание и полный путь к зараженному файлу.*

*Ниже, в группе****Действие****, приводится описание заражения файла (в данном случае написано, что файл заражен вирусом EICAR и лечение его невозможно). Рядом расположены кнопки:****Лечить****,****Удалить****,****Пропустить****. Поскольку вылечить EICAR нельзя, то первая кнопка неактивна.*

*Вы можете либо пропустить, либо удалить eicar.com. Поскольку как уже говорилось ранее, все зараженные файлы удаляются не насовсем, а всего лишь перемещаются в изолированное резервное хранилище, в случае невозможности лечения рекомендуется выбирать удаление.*

Нажмите **Удалить (напоминаю, что в зависимости от установленного у вас пакета, окна и действия могут отличатьсяот указанных в тексте работы)**

1. После того как Вы выбрали действие, **Антивирус** применит его к инфицированному файлу, в данном случае - удалит eicar.com. Это сразу же отобразится в окне статистики. Изучите представленные в нем данные и нажмите **Закрыть**
2. Проверьте, что удаленный файл eicar.com появился в резервном хранилище.
3. Ознакомьтесь с внешним видом окна резервного хранилища. Для того, чтобы получить управление над каким-либо объектом из резервного хранилище, его нужно выделить.

Выделите строку " Заражен: вирус EICAR-Test-File "

1. Как только был выбран объект, стали активными кнопки управления им: **Удалить** и **Восстановить**. Напомним, что восстанавливать файлы из резервного хранилища настоятельно не рекомендуется.

Удалите eicar.com, нажав **Удалить (напоминаю, что в зависимости от установленного у вас пакета, окна и действия могут отличатьсяот указанных в тексте работы)**

1. Убедитесь, что резервное хранилище теперь пусто и закройте окно статистики, нажав **Закрыть**

**Задание 3. Лечение инфицированных файлов**

*Выполнив задание 2, можно с уверенностью сказать, что установленный****Антивирус*** *обнаруживать вирусы умеет. Теперь нужно проверить, умеет ли он лечить. Это можно сделать, повторив действия предыдущего задания, только для излечимого тестового вируса**CURE-EICAR. Однако мы поступим иначе. Проверим, как работает постоянная защита, а именно ее**компонент, отвечающий за проверку файловой системы.*

Для этого нужно включить постоянную защиты и затем попытаться получить *доступ* к *cure*-eicar.com.

**Отчет. Скрины выполнения следующих пунктов: №2, 5, 7, 8, 9, 10**

1. Включите постоянную защиту антивируса .
2. Откройте папку Test.

Поскольку ранее в задании 2, на шаге 4, было дано указание удалить файл eicar.com, а не пропустить, в папке осталось только два файла, *cure*-eicar.com и susp-eicar.com

1. Поскольку постоянная защита ответственна за проверку всех файлов "на лету", она должна перехватить наше обращение к *cure*-eicar.com, на лету вылечить и отдать нам только то, что осталось. В данном случае - 4-байтный файл, содержащий "*CURE*" . Проверим это.
2. Обратитесь в файлу *cure*-eicar.com, один раз щелкнув по нему курсором мыши и не задевая иконку файла susp-eicar.com
3. **Антивирус** сразу же должен обнаружить, что Вы пытаетесь обратить к зараженному файлу. Как результат - выводится окно с запросом действия, которое нужно применить к найденному вирусу8
4. Вылечите файл *cure*-eicar.com, нажав **Лечить**
5. Проверьте, что оставшийся в папке Test файл *cure*-eicar.com имеет размер всего 4 байта
6. Убедитесь, что перед лечением файл был помещен в резервное хранилище.
7. Проверьте, что теперь резервное хранилище содержит *cure*-eicar.com, причем его размер равен 73 байтам
8. Очистите резервное хранилище.

**Задание 4. Помещение файлов на карантин**

*Как видно из предыдущих заданий, перед каждым своим вмешательством****Антивирус*** *копирует исходный**файл в специальную защищенную папку, называемую резервным хранилищем. Из нее файлы рекомендуется только удалять, поскольку они или признаны инфицированными и при этом неизлечимыми, или были успешно вылечены и следует использовать их вылеченную копию.*

*В этом задании изучается второе хранилище****Антивируса****, карантин.*

*На карантин ставятся все подозрительные файлы - то есть такие, которые по всем признакам инфицированы, но вердикт об их неизлечимости пока не вынесен. Может быть, при следующем обновлении антивирусных баз в них будет добавлена**информация, позволяющая это сделать, или же свидетельствующая о неизлечимости. В первом случае можно будет провести повторную проверку карантина и вылечить теперь уже допускающие лечение файлы, во втором - удалить с перемещением в резервное хранилище.*

*Еще одно отличие карантина от резервного хранилища состоит в том, что на карантин можно ставить объекты вручную, например если они у пользователя все же вызывают подозрения, несмотря на отрицательный ответ антивируса.*

**Отчет. Скрины выполнения следующих пунктов: №2, 3, 4, 6**

1. Дайте постоянной защите обнаружить последний из созданных в первом задании тестовый вирус SUSP-EICAR. Для это повторите действия предыдущего задания, но относительно файла susp-eicar.com.
2. **Антивирус** просканирует этот файл и обнаружит его подозрительным. В результате выведется окно с просьбой выбрать необходимое действие.

Вам будет предложено три варианта: поместить на карантин, удалить или пропустить. Поскольку файл признан подозрительным, лечение невозможно (иначе бы было предложено его сначала вылечить).

Нажмите **Карантин**

1. Обратите внимание, что после помещения susp-eicar.com на карантин, в папке Test остался только вылеченный в предыдущем задании *cure*-eicar.com
2. Теперь проследите, что susp-eicar.com появился на карантине. Обратите внимание на сводную статистику по карантину.
3. Вспомните, что для файлов, которые антивирус помещал в резервное хранилище вердикт был однозначен - заражен. В карантин же помещаются файлы с более мягким статусом - **возможно** заражен. Таким образом, помещение на карантин подразумевает, что в дальнейшем этот вердикт может быть изменен. А изменен он может быть только при проверке с другими, более новыми или полными антивирусными базами. Поэтому по умолчанию после каждого обновления антивирусных баз все файлы на карантине перепроверяются, а для запуска перепроверки вручную на закладке **Карантин** есть кнопка **Проверить все** и контекстное меню любого объекта карантина содержит пункт **Проверить**
4. Выделите строку с susp-eicar.com и щелкнув на нем правой клавишей мыши, выведите контекстное меню. Закройте окно статистики, нажав **Закрыть**