Практическая работа_Создание и модификация тестового вируса, тестирование антивирусной функциональности

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 «вируса» 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.

Задание 1.

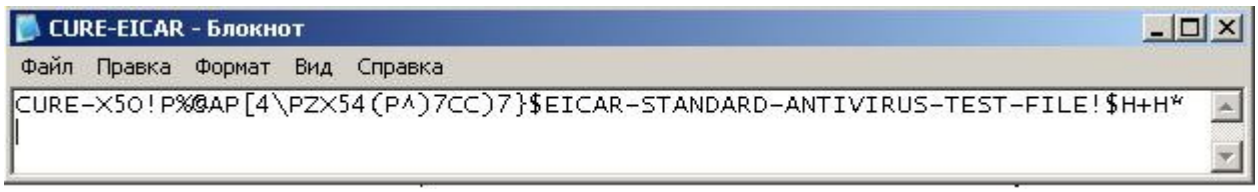
Создайте 3 файла (Вирус1, Вирус2, Вирус3): скопируйте строку символов в Блокнот, сохранив один файл с расширением ***.com****, а другой - с расширением* ***.txt****. Третий файл создается путем* ***архивирования*** *одного из созданных файлов.*

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.

Задание 2*.*

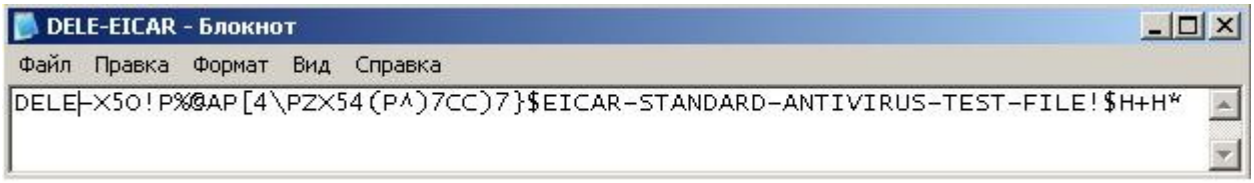
Создать файл CURE-EICAR (Вирус4). Файл создается в Блокноте путем добавления в начало вируса символов ***"CURE-"*** *и сохранения файла с расширением* ***.com.*** *Обнаружив такой файл антивирус «вылечит» его, сократив размер файла до 4 байт (символы «CURE»).*



Модификация вируса CURE-EICAR

Задание 3.

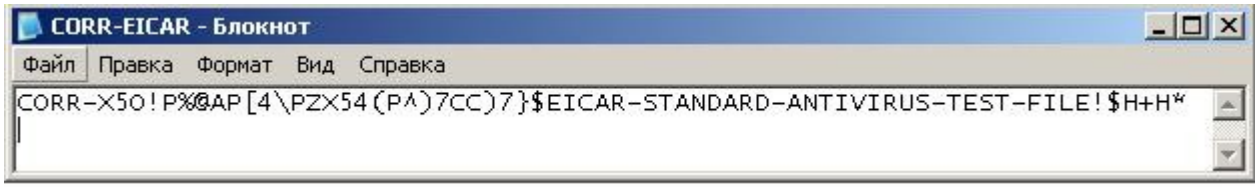
Создать файл DELE-EICAR (Вирус5). Файл создается в Блокноте путем добавления в начало вируса символов ***"DELE-"*** *и сохранения файла с расширением* ***.com.*** *Обнаружив такой файл, антивирус определяет его как неизлечимый или троянскую программу и удаляет. По результатам проверки файл должен остаться только в резервном хранилище.*



Модификация вируса DELE-EICAR

Задание 4.

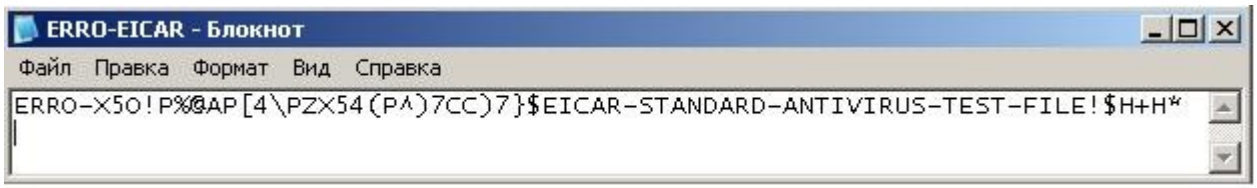
Создать файл CORR-EICAR (Вирус6). Файл создается в Блокноте путем добавления в начало вируса символов ***"CORR-"*** *и сохранения файла с расширением* ***.com.*** *Обнаружив такой файл, антивирус определяет его как файл с поврежденной структурой, вследствие чего проверить его на наличие вирусов невозможно. Такой файл признается условно чистым.*



Модификация вируса CORR-EICAR

Задание 5.

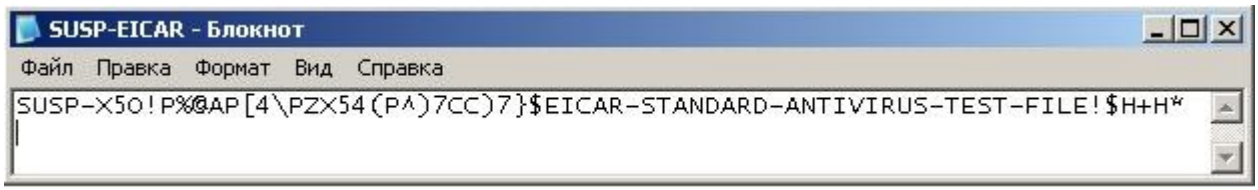
Создать файл ERRO-EICAR (Вирус7). Файл создается в Блокноте путем добавления в начало вируса символов ***"ERRO-"*** *и сохранения файла с расширением* ***.com.*** *При сканировании такого файла, антивирус обнаружит ошибку при анализе его содержимого (например, при нарушении целостности при проверке многотомного архива). Такой файл признается условно чистым.*



Модификация вируса ERRO-EICAR

Задание 6.

Создать файл SUSP-EICAR (Вирус8). Файл создается в Блокноте 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.*



Модификация вируса SUSP-EICAR

Задание 7.

Создать файл WARN-EICAR (Вирус9). Файл создается в Блокноте 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.*

Задание 8.

Произведите проверку каждого из созданных 9 файлов-«вирусов» всеми сервисами онлайн-проверки поочередно.

1. https://virusdesk.kaspersky.ru/

2. https://vms.drweb.ru/scan_file/

3. https://2ip.ru/antivirus/

4. http://www.virscan.org/language/en/

5. https://www.virustotal.com/gui/home

Для сканеров по первым трем ссылкам скопируйте полученный результат в файл.

Для сканеров по ссылкам 4) и 5) укажите, какое количество сканеров обнаружило вирус, сколько (и какие) сканеры вирус не определили.