1. Министерство высшего образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 5**

«**анализ вредоносных программных средств**»

1. по дисциплине «Основы Информационной Безопасности»
2. Выполнил
3. студент гр. Белоконь Д. А.
4. <*подпись*>

Проверил Пахомов М. А.

1. <*подпись*>

1. Санкт-Петербург
2. 2023
3. **Цель работы**

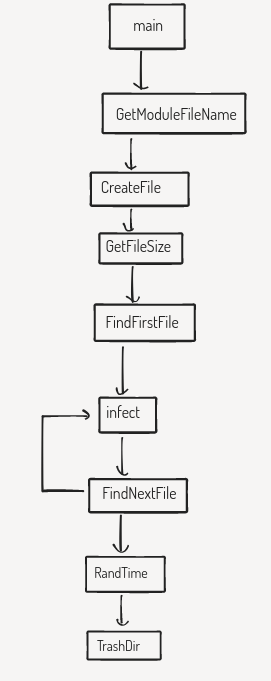
Приобретение практических навыков по противодействию вредоносным программным средствам на примере компьютерных вирусов.

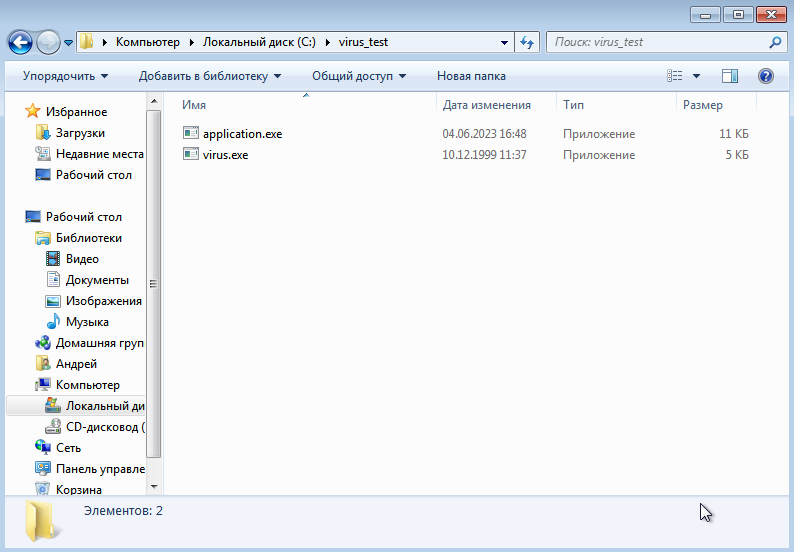
Формулировка задания

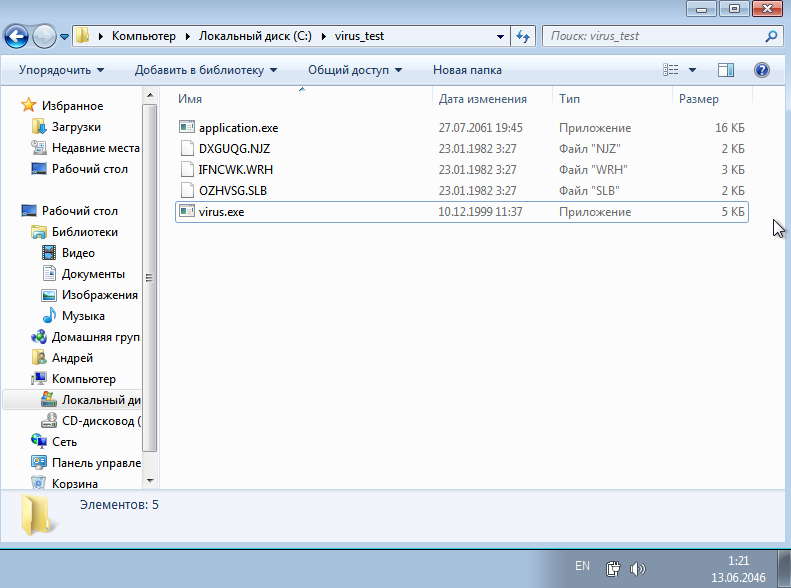
Необходимо с помощью двух генераторов вирусов создать соответствующие тестовые программы и проанализировать их поведение и устройство.

Результаты

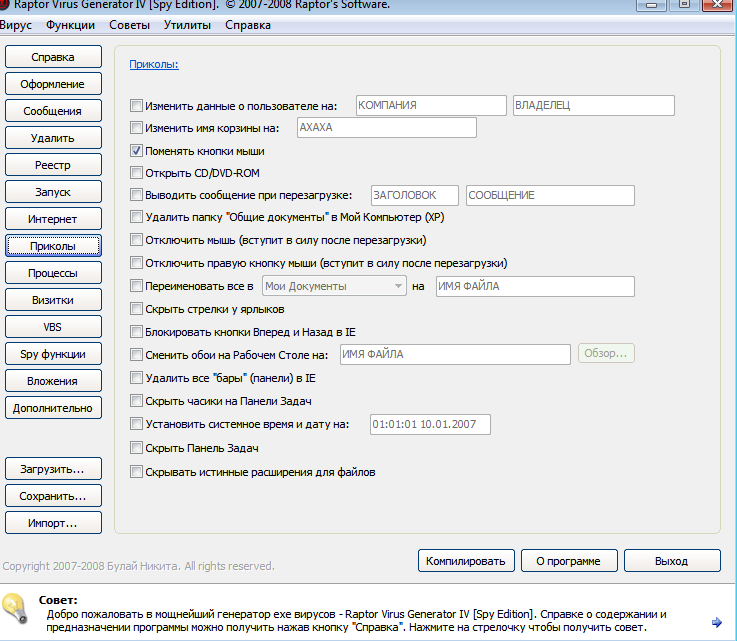
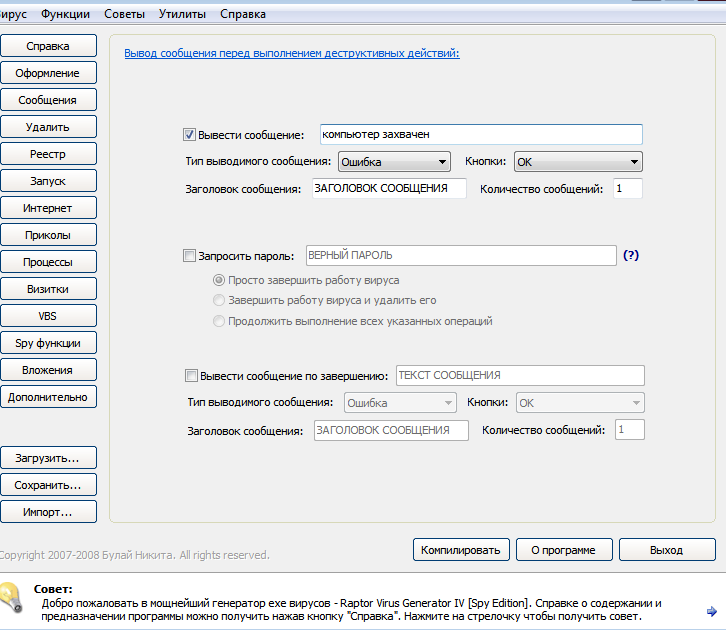
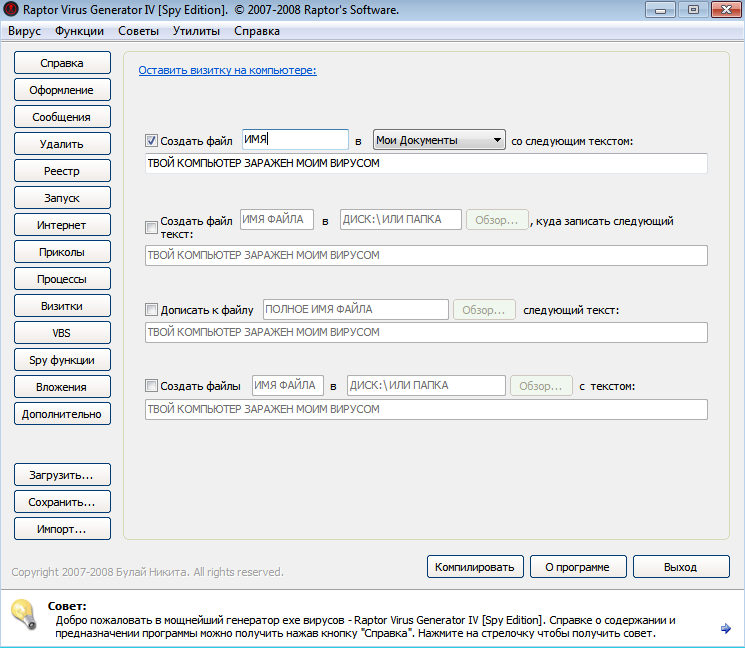
Для начала, как и указано, поставим виртуальную машину и создадим директории virus\_test и virus\_disk\_test. Последнюю примонтируем к диску X.

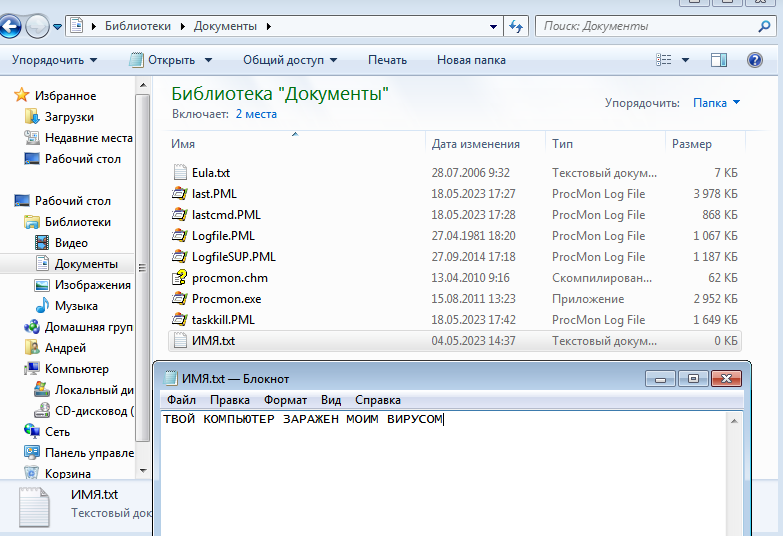
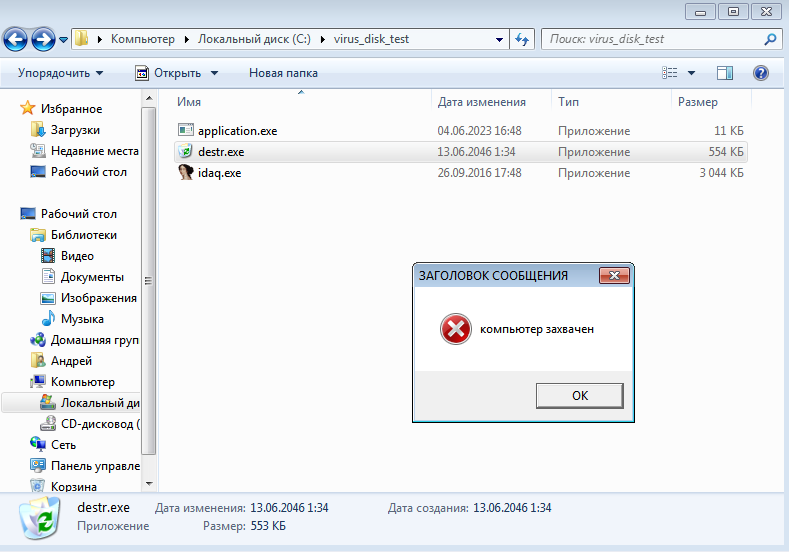
Затем через GVDG сделаем вирус с единственными функциями, которые можно увидеть на скриншоте: «Намусорить в текущем каталоге» и «Установить случайное время».

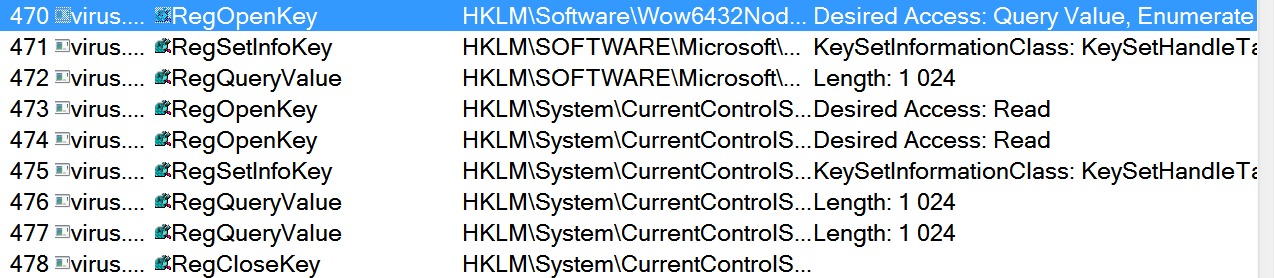
После копируем вирус в отдельную папку и запускаем:

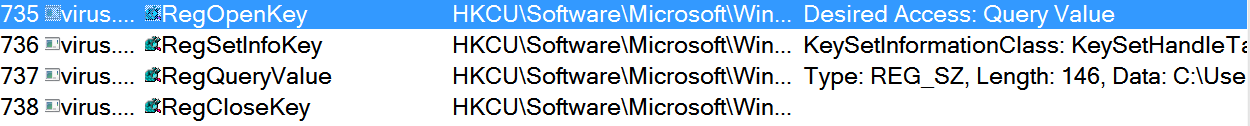


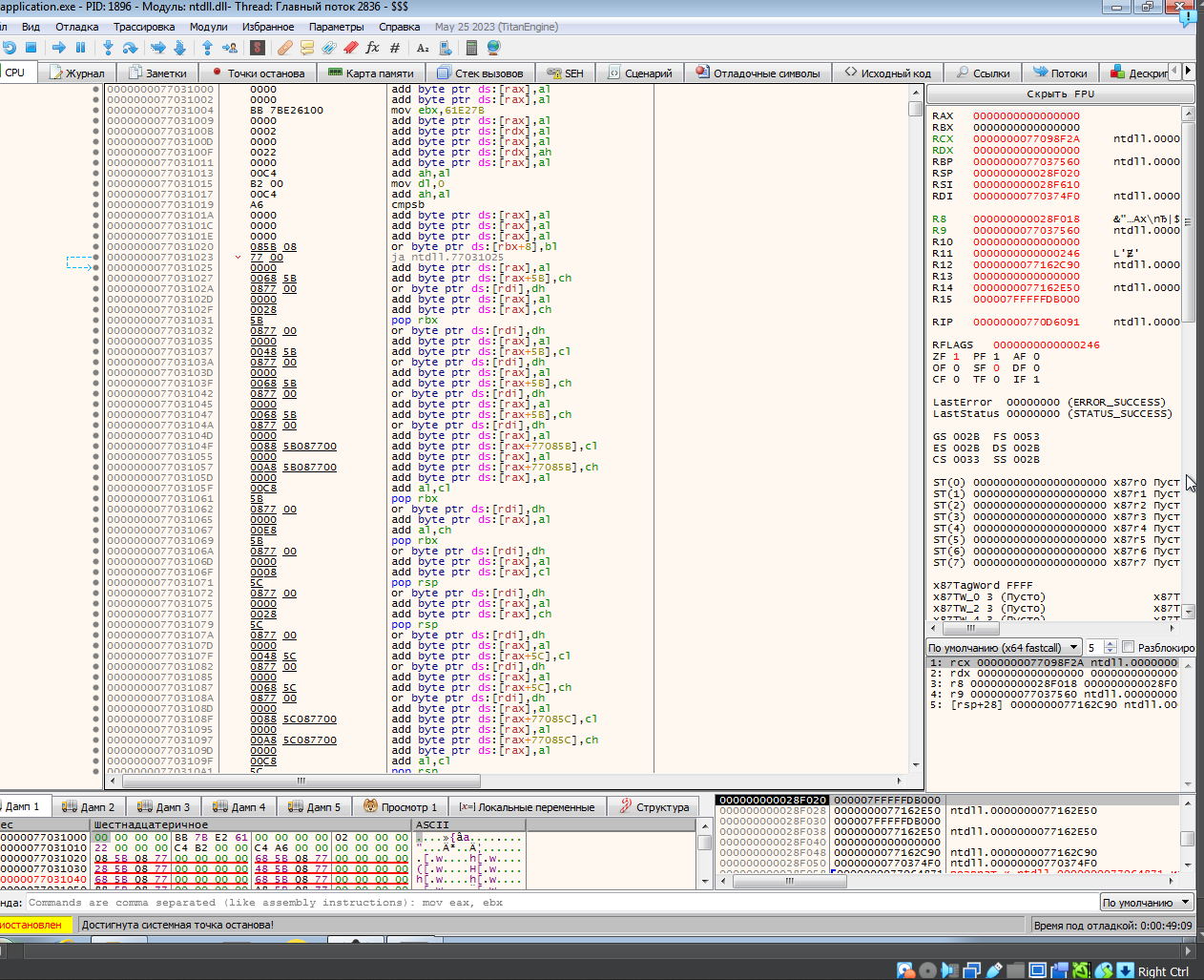
Логично, что Total Commander показывает, что соседний файл изменён. При запуске рядом лежащего файла происходит то же, что и на скриншотах выше. Лечение же заражённого файла также происходит успешно, то есть вирус не перезаписывает всю программу, а просто добавляет себя в неё. Лежащий в файлах антивирус 360 показывает, что вируса в программе нет.

Далее поработаем со вторым генератором вирусов:

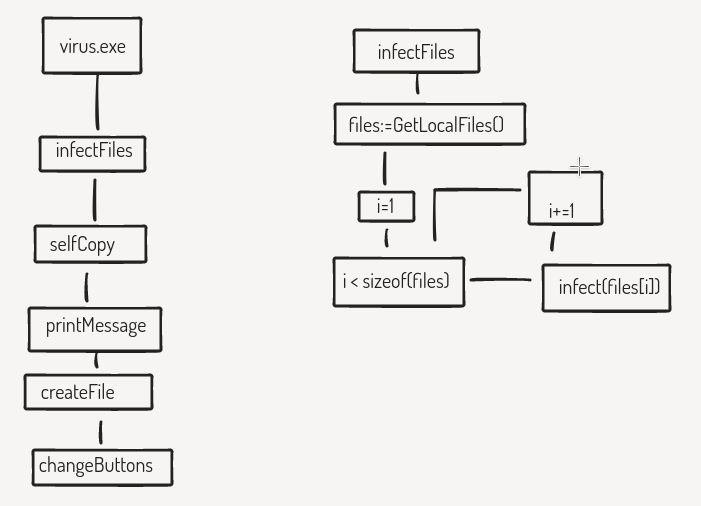
Вирус отрабатывает так:

Откроем apiMonitor и выделим предполагаемые деструктивные функции. Изменение клавиш мыши:

Вызов системного сообщения:

Дизассемблированная заражённая программа. Участок, по предположению заражающий другие файлы:

По итогу анализа второго вируса можем составить подобную блоксхему:



Вывод

Это было трудным погружением в анализ работы компьютерных вирусов. В основном, за счёт того, что работа происходила на старой ОС Windows на виртуальной машине, что осложняло взаимодействие с её элементами.