**РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное автономное образовательное учреждение

высшего образования

«Санкт-Петербургский политехнический университет Петра Великого»

(ФГАОУ ВО «СПбПУ»)

**Институт среднего профессионального образования**

**Отчёт по лабораторной работе №6**

**по учебной дисциплине «МДК04.02»**

**Тема: «Составление документа «Вирусы»»**

Выполнил студент

группы 219/21

Чиликин Александр Александрович

Преподаватель

Иванова Дарья Васильевна

Санкт-Петербург,

2025

**Цель работы:** изучить типы различных вирусов, их принцип работы, особенности и т.д.

**Задачи:**

1. Разархивировать вирус
2. Запустить вирус
3. Найти подозрительные процессы
4. Удалить вирус
5. Проверить компьютер с помощью антивируса

**Майнер**

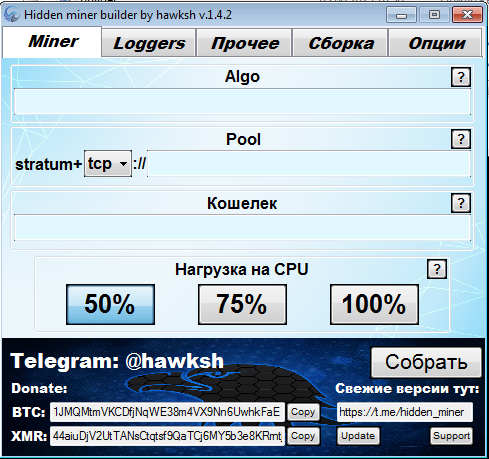


Рисунок 1 - Меню майнера

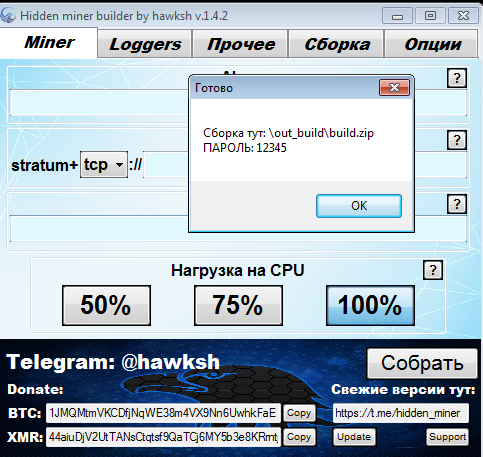


Рисунок 2 - Сборка завершилась

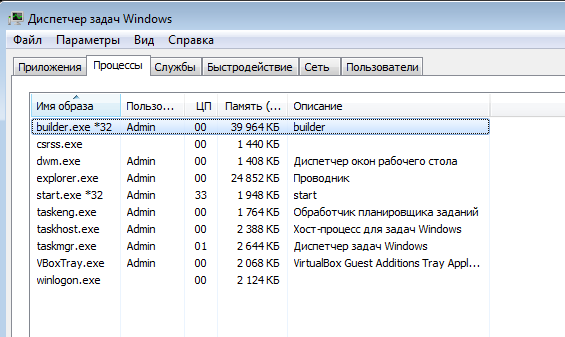


Рисунок 3 – Запускаем, в диспетчере задач появляется новый процесс «start.exe \*32»

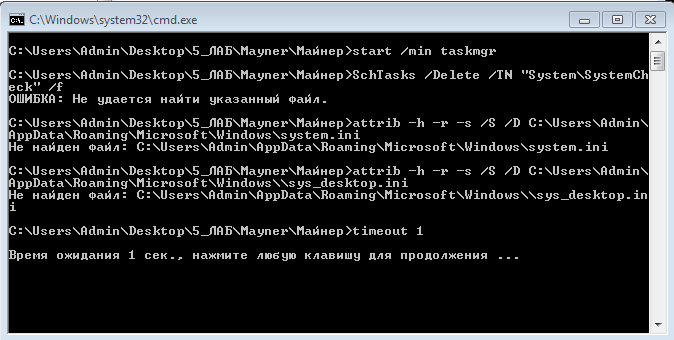


Рисунок 4 - Удаляем

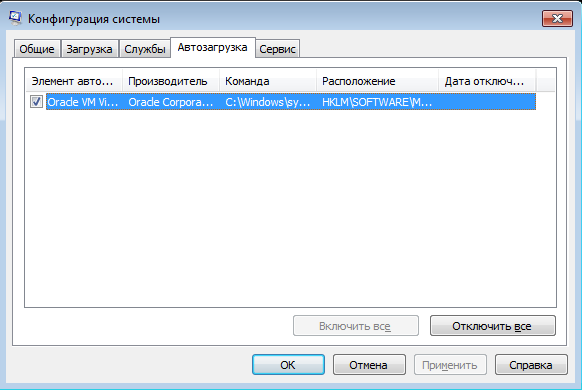


Рисунок 5 – в автозагрузке майнера нет

**Вирус petya**

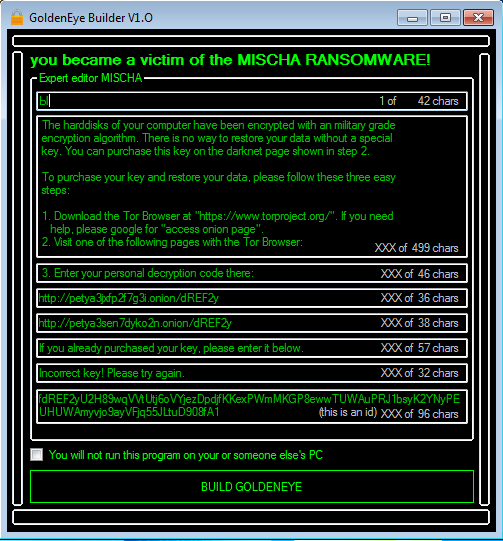
****

Рисунок 6 – Билдер пети

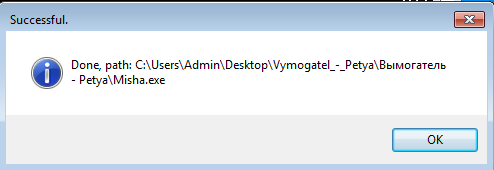


Рисунок 7 – все прошло успешно

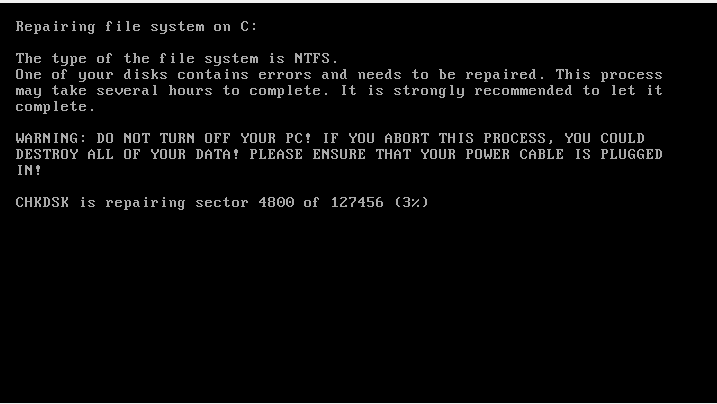


Рисунок 8 – шифровка файлов

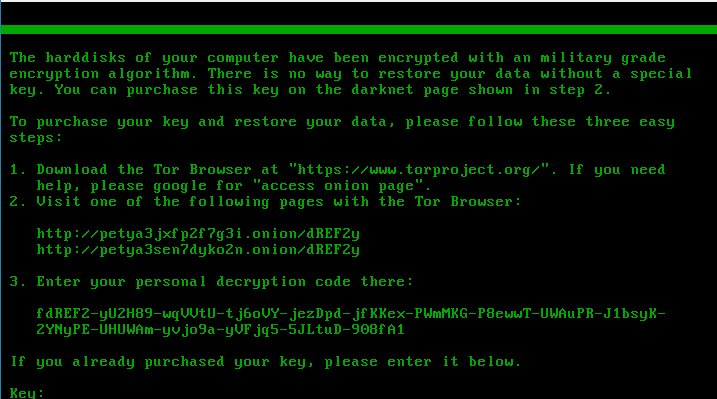


Рисунок 9 – надо ввести ключ

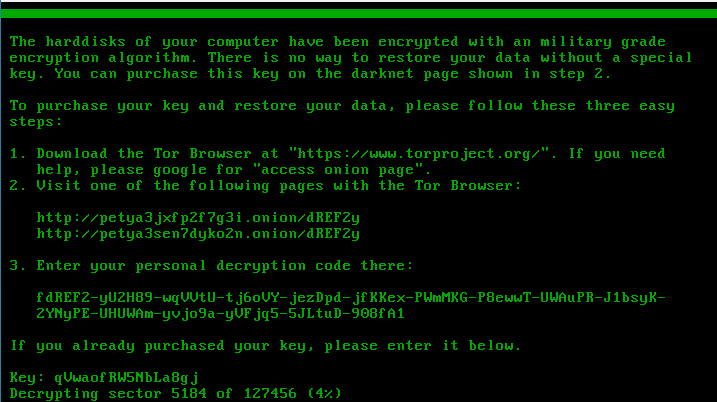


Рисунок 10 – ввели ключ



Рисунок 11 – Петя просит перезапустить компьютер, после перезапуска ПК выясняется что файлы повреждены и запуск не возможен.

**Вирус WinLocker**

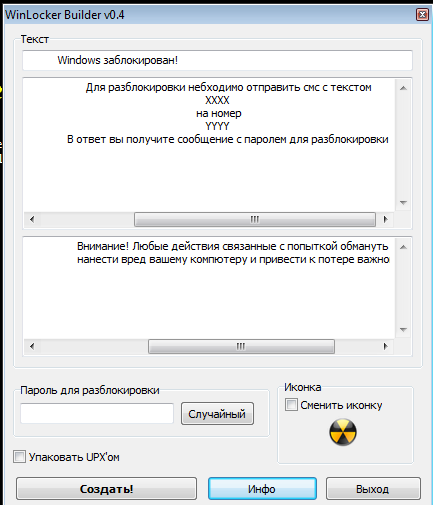


Рисунок 12 – запускаем билдер

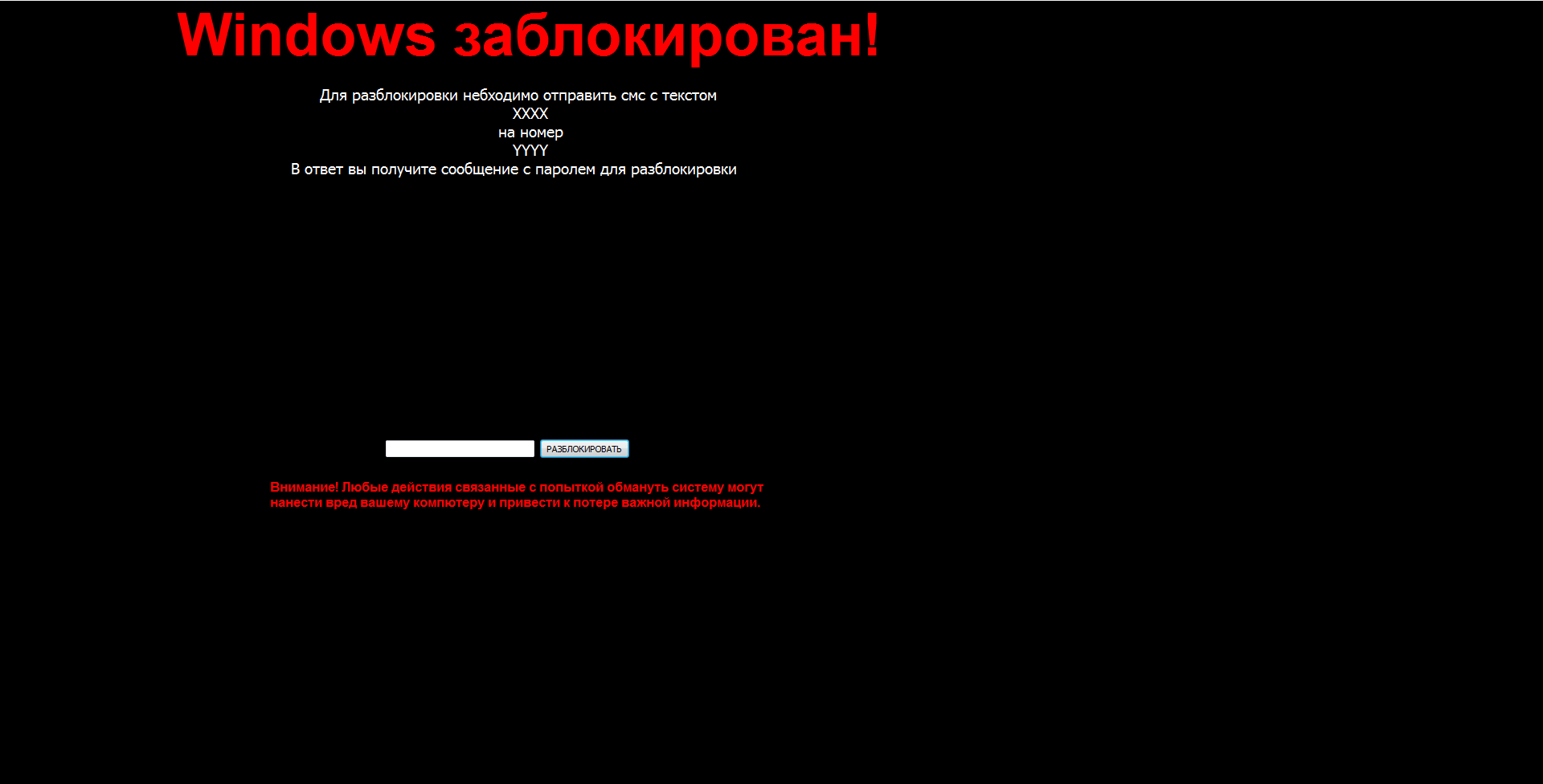


Рисунок 13 – WinLocker начал работать

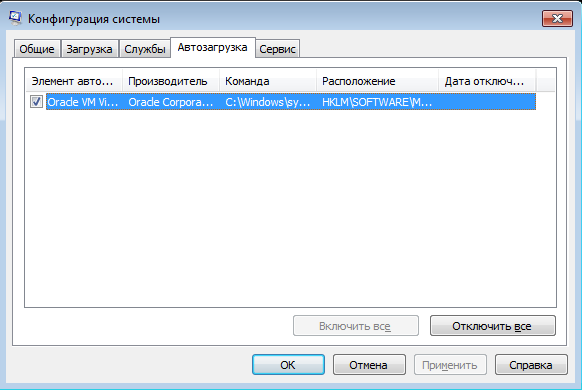


Рисунок 14 – в автозагрузке нет вируса

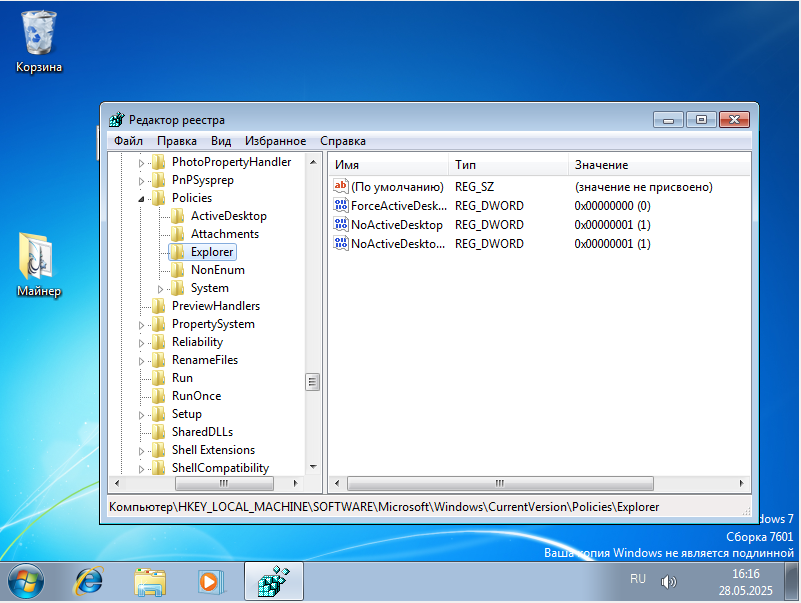


Рисунок 15 – Отсутствует папка Run

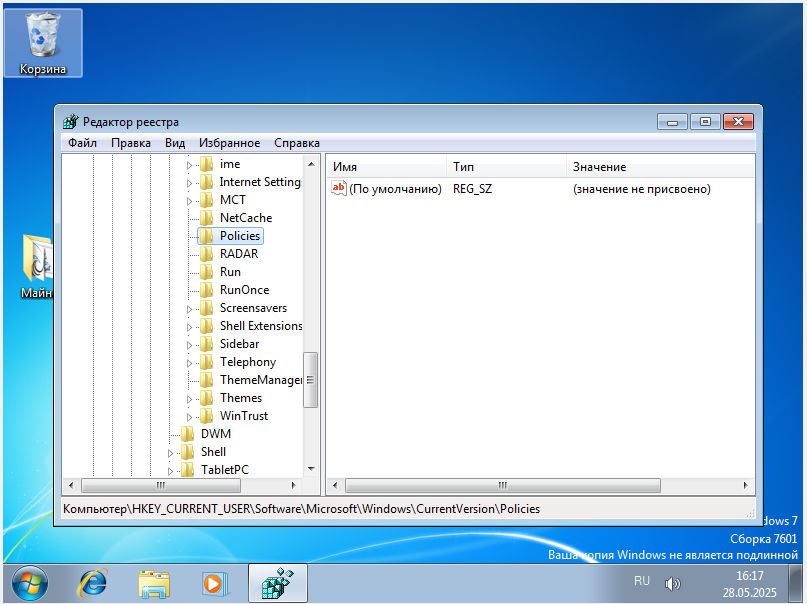


Рисунок 16 – в папке Policies отсутствуют папки Explorer и Run

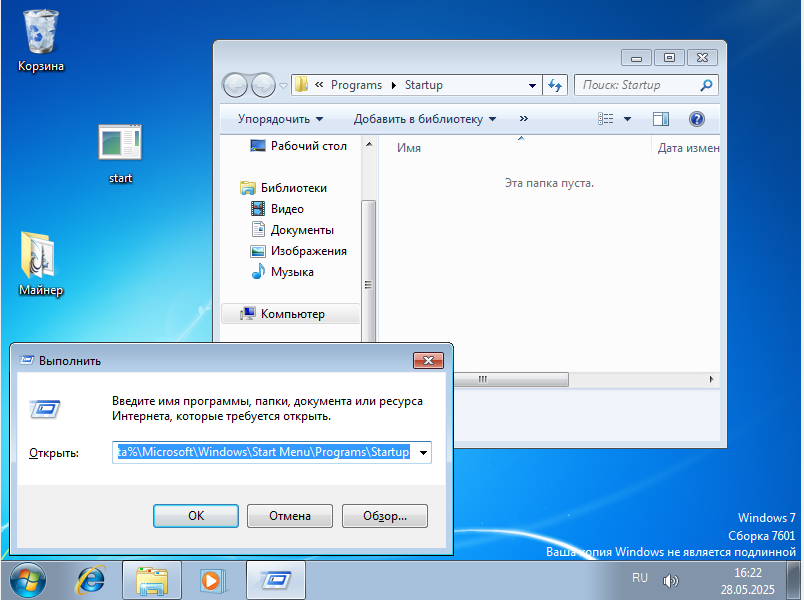


Рисунок 17 – в папке StartUp ничего нет

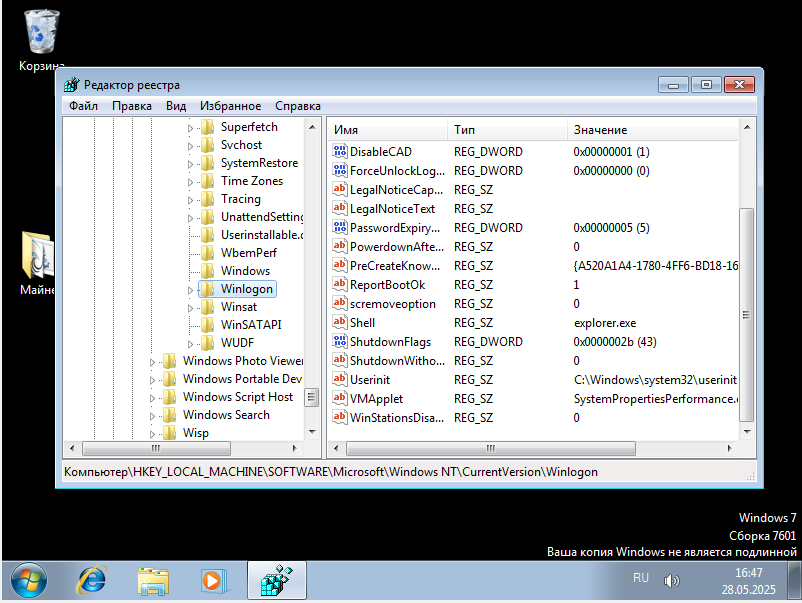


Рисунок 18 – в shell остался explorer.exe

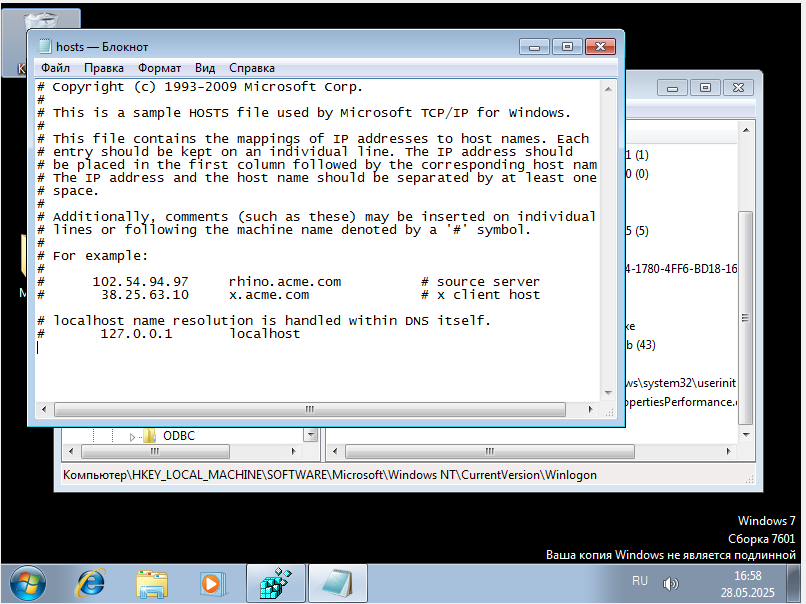


Рисунок 19 – в файле host изменений нет

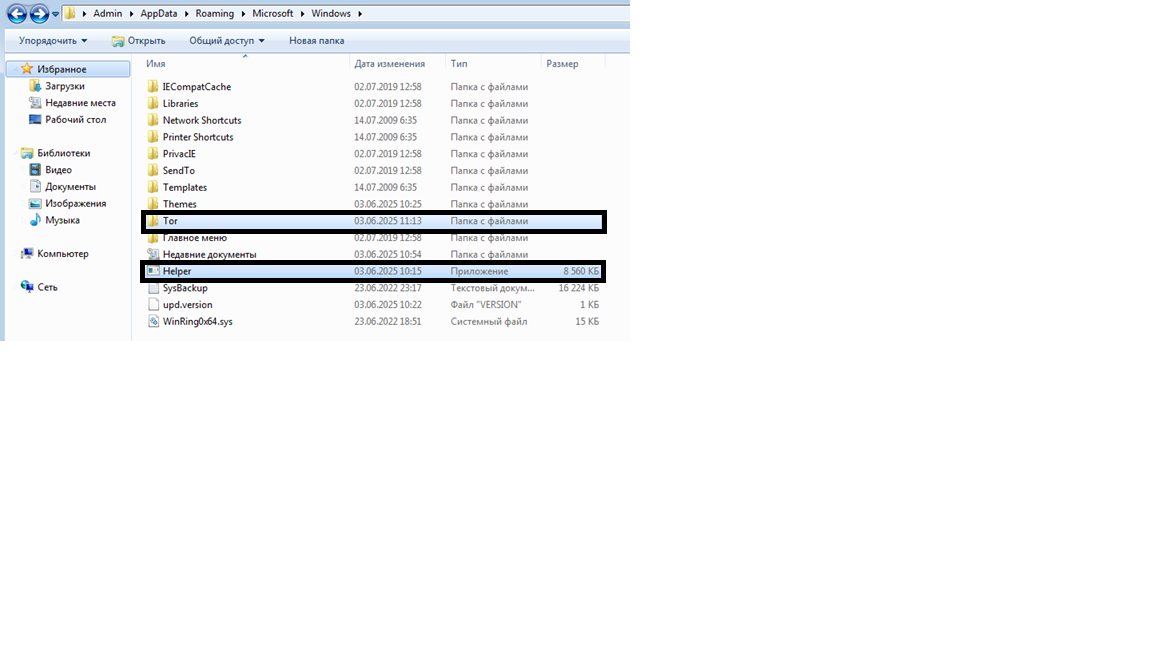


Рисунок 20 – после майнера остался файл Helper.exe и папка Tor

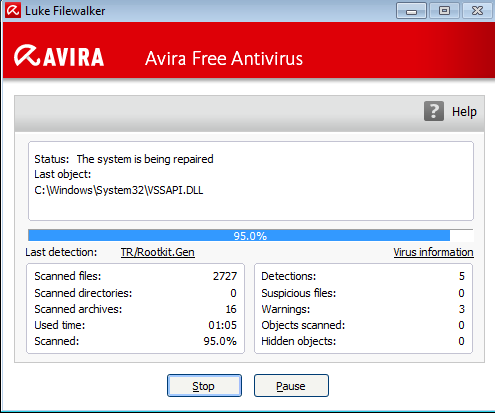


Рисунок 21 – включаем антивирус и удаляем то что осталось от вирусов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Название вируса | По среде обитания | По способу заражения | По деструктивным возможностям (по способам воздействия) | По особенностям алгоритма вируса |
| Petya | Файлово-загрузочный | Резидентный | Очень опасный | Червь |
| WinLocker | Системный | Резидентный | Очень опасный | Простейший |
| Майнер | Файловый | Резидентный | Опасные | Стелс-вирус |