МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ОТКРЫТЫЙ КОСМИЧЕСКИЙ ЛИЦЕЙ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА ЛЕТЧИКА-КОСМОНАВТА ГЕОРГИЯ ТИМОФЕЕВИЧА БЕРЕГОВОГО» МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОДСКОЙ ОКРУГ СИМФЕРОПОЛЬ РЕСПУБЛИКИ КРЫМ

Создание антивирусной утилиты для очистки от вредоносного ПО ОС Windows

Работу выполнил: ученик 10-А класса МБОУ «Открытый Космический Лицей» имени Г.Т. Берегового

Аметов Салим

Симферополь, 2026 г.

Актуальность

- Стандартные антивирусы не могут работать в среде восстановления ОС Windows. Для восстановления системы после воздействия вредоносного ПО компании выпускают загрузочные диски или флешки. При этом, они не гарантируют полноценного востановления системы или файлов, в большинстве случаев ОС приходится переустанавливать, как и часть программ, установленных на системном диске.
- Поэтому давно назрела потребность в программах, включающих в себя обе функции, сведенные при этом в единый бинарный файл с интуитивно понятным интерфейсом.

Цели проекта

Цель проекта: создать программу с набором утилит для устранения вирусов и их последствий.

Для достижения этой цели нужно выполнить следующие задачи:

1) Создать компонент по управлению автозагрузкой.
2) Создать простой файловый менеджер для базовых операций.
3) Создать менеджер процессов, который может изменить «критичность» процесса.
4) Реализовать работу с реестром для снятия ограничения групповых политик и сделать автозагрузку реестра в среде восстановления.
5) Объединить все компоненты в одну независимую программу, с набором защит от внешних воздействий другого ПО.

Объект исследования: Вредоносные программы в среде ОС Windows.

Предмет исследования: файлы, процессы, определённые параметры реестра ОС Windows.

Полученный результат: один бинарный файл, способный работать не только в обычной среде, но и в среде восстановления, без дополнительных программ.

Что из себя представляет данный проект?

Антивирус Монтировка – это набор антивирусных утилит направленных на устранение не только самих вирусов, но и их последствий.

Программа включает в себя следующие

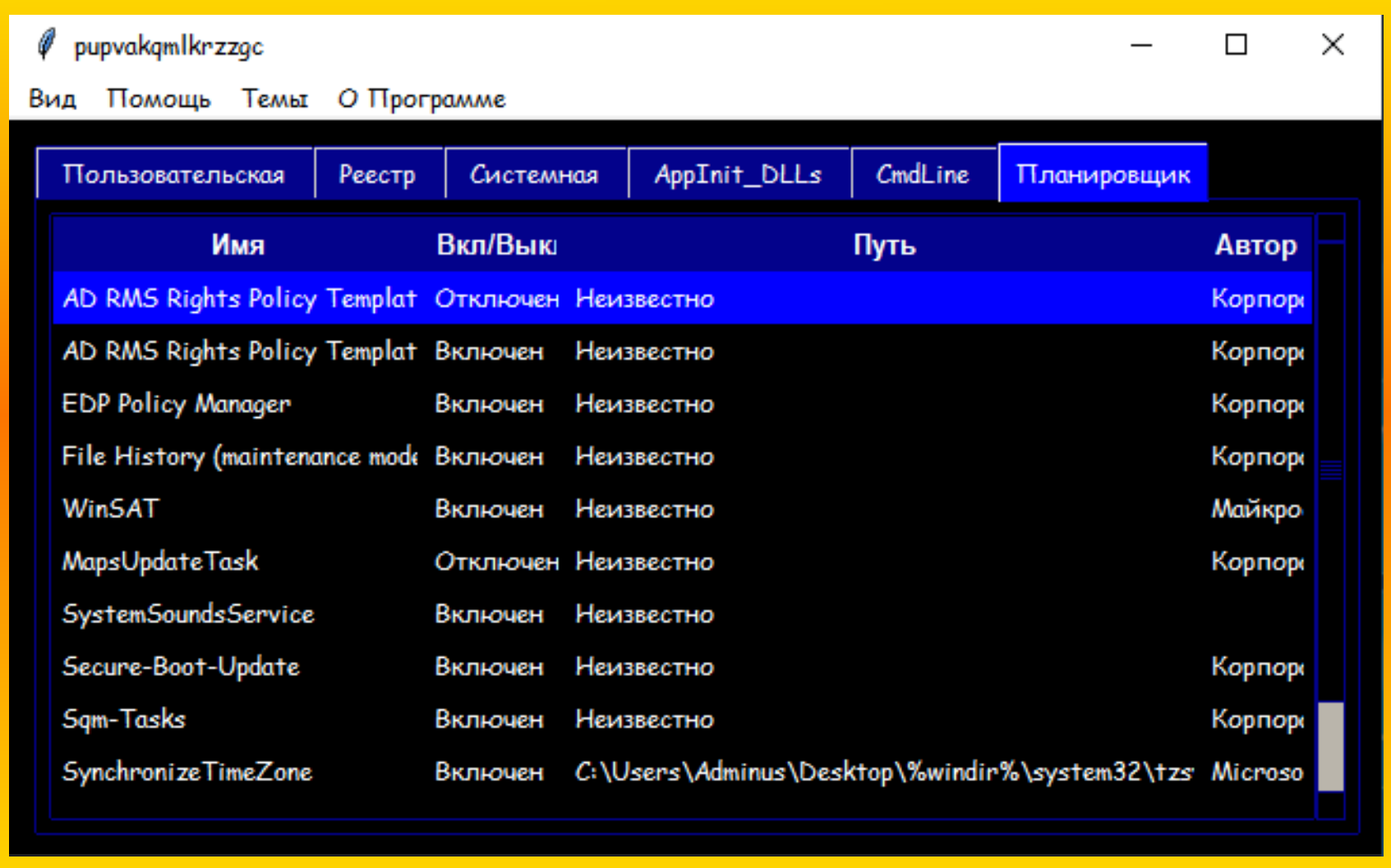
Компоненты:

- ***Мастер Автозагрузки***
- ***Менеджер Процессов***
- ***Файловый Менеджер***
- ***Разблокировка Всего***
- ***Прочие мелкие утилиты***

Описание программы

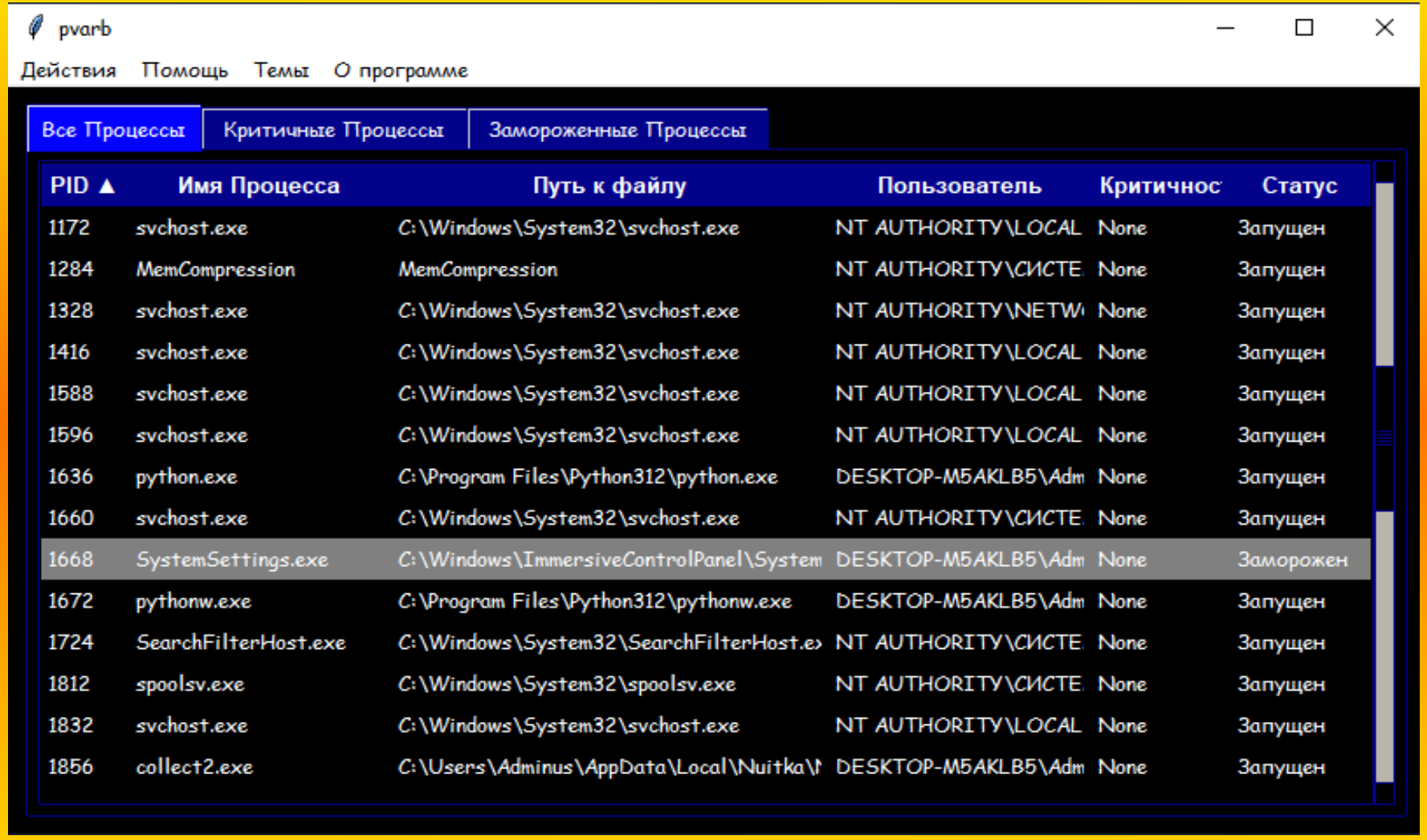
- Программа написана на Python 3.12
- Программа работает на Windows 10 и 11.
- Всего строчек кода более 7700.
- Вес итогового бинарного файла не превышает 18 МБ.
- Потребляет около ~22 МБ ОЗУ.
- Скомпилированная программа не требует дополнительных библиотек и папок с файлами.
- Программа является одним файлом: если ей нужно будет создать дополнительный файл (файл со списком исключений), то она его автоматически создает.

Мастер Автозагрузки



Компонент, позволяющий управлять всеми видами автозагрузки

Менеджер Процессов

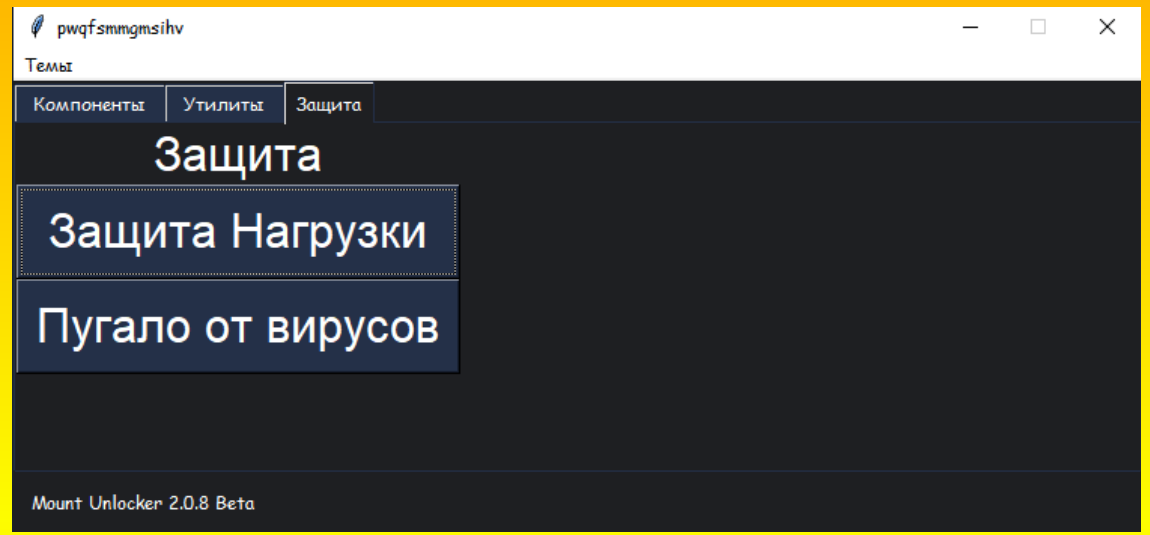


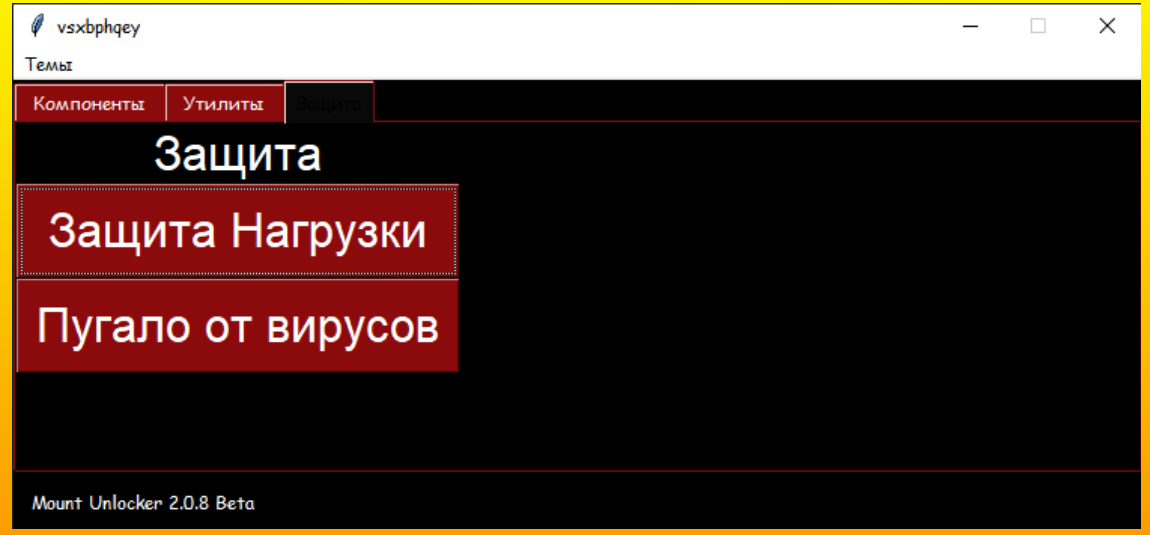
Компонент, позволяющий закрывать, замораживать, размораживать и изменять «критичность процесса»

Файловый Менеджер

Компонент, позволяющий проводить все базовые операции с файлами

Работоспособность в среде восстановления





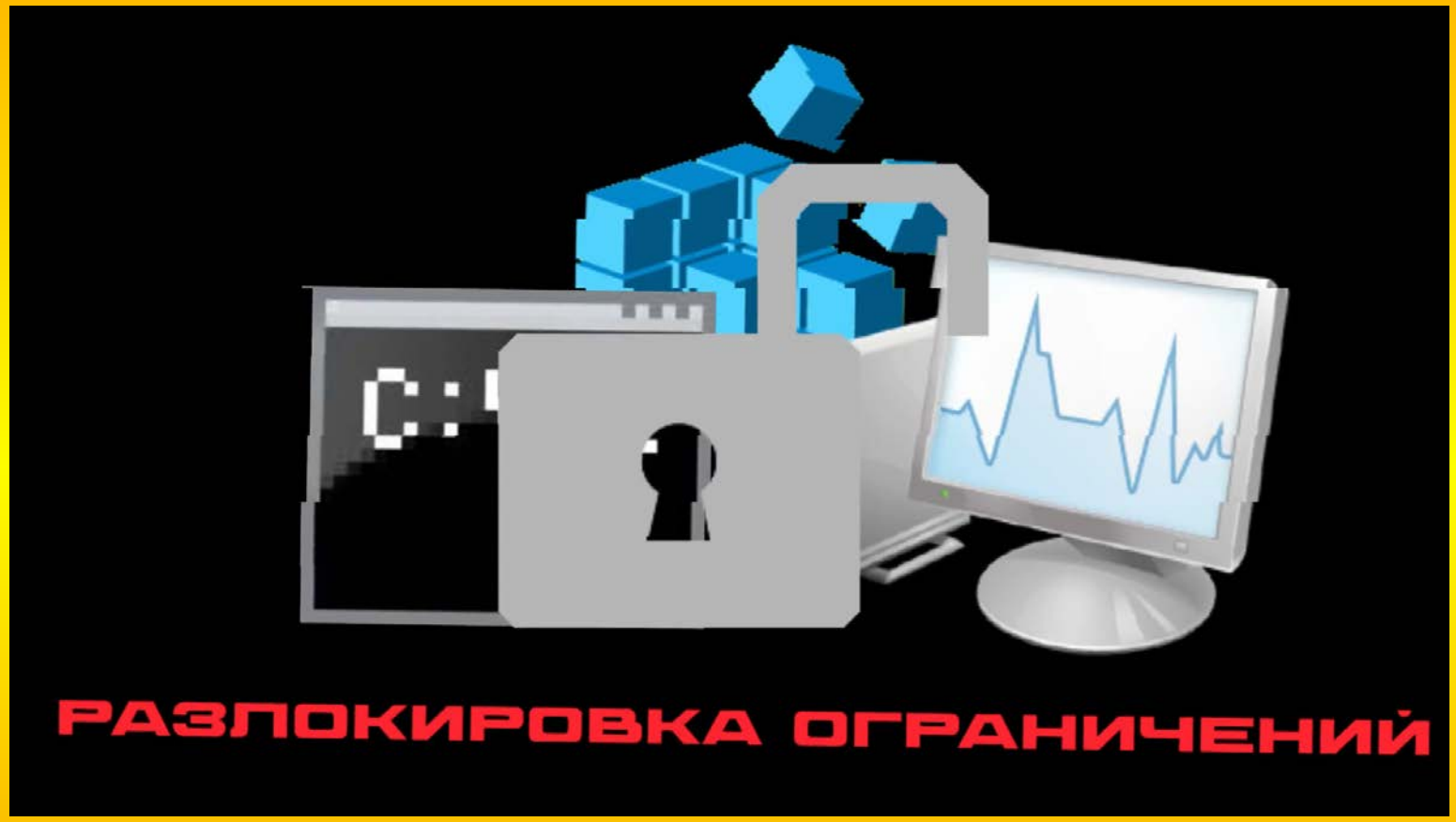
Программа автоматически определяет том диска, на котором установлена Windows и загружает с него реестр, чтобы была возможность отредактировать автозагрузку в среде восстановления.

Это позволяет удалить вредоносное ПО, не запуская основную систему и без использования флешек.

Защита Нагрузки

Данный компонент представляет из себя сканер процессов - если процесс имеет подозрительное название или избыточно нагружает систему, то он будет приостановлен для дальнейших действий.

Разблокировка Всего



В программе есть функция, позволяющая автоматически отредактировать групповые политики Windows, ради снятия ограничений на запуск ПО из-за воздействия вирусов.

Также Программа включает в себя следующие Компоненты:

- «Пугало» от вирусов:

  Имитирует наличие определённого ПО на ПК, из-за которого снижается вероятность запуска вируса стиллера.
- Запуск от имени администратора:

  Позволяет запустить файл от имени администратора.
- Перезагрузка ПК:

  Позволяет выполнить перезагрузку ПК, даже если она заблокирована через групповые политики.
- Замена Setch и Utilman:

  Позволяет заменить редко используемые системные файлы на любую другую программу для маскировки и запуска внутри основной системы. Восстановить эти системные файлы можно одной кнопкой.

Итоги

В результате данного проекта, удалось разработать программу, которая может:

1) работать в среде восстановления;
2) управлять автозагрузкой;
3) управлять запущенными процессами процессами не только вручную, но и полуавтоматически;
4) управлять файлами;
5) разблокировать ограничения в системе;
6) симулировать различное ПО;
7) прочие мелкие возможности.

Полученный бинарный файл позволяет намного проще удалять вирусы и их последствия на ОС Windows.