**Федеральное агентство связи**

**Ордена Трудового Красного Знамени**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Московский технический университет связи и информатики»**

**Отчет по разработке комплекса антивирусной защиты**

по дисциплине «Защита информации от вредоносного ПО»

Выполнил студент БВТ1802

Денисович Л.С.

Руководитель

Барков В.В.

Москва 2021

Цель: разработать программный комплекс антивирусной защиты согласно техническому заданию.

**Требования для запуска программного комплекса**

ОС Windows 10 64-bit

**Средства межпроцессного взаимодействия**

Для обмена данными между клиентским и серверным приложениями используются почтовые ящики.

Коды операций, которые клиентское приложение посылает серверному приложению для осуществления действия, выбранного пользователем.

enum class CMDCODE : uint8\_t

{

SERVERSHUTDOWN = 0, CLIENTSHUTDOWN, SCAN, STOPSCAN, DELETETHREAT, QUARANTINE, UNQUARANTINE,

MONITOR, STOPMONITOR, SCHEDULESCAN, CANCELSCHEDULESCAN

};

Коды типов данных для пересылки между приложениями

enum class TYPECODE : uint8\_t

{

UINT8 = 0, UINT16, UINT32, UINT64,

INT8, INT16, INT32, INT64,

FLOAT32, FLOAT64,

U16STRING, U16CHAR,

STRUCT,

AUINT8, AUINT16, AUINT32, AUINT64,

AINT8, AINT16, AINT32, AINT64,

AFLOAT32, AFLOAT64

};

**Формат хранения вредоносных сигнатур в антивирусных базах**

Антивирусные базы хранятся в бинарном файле. В качестве заголовка данного файла используется фамилия студента на латинице (“Denisovich”). Данный заголовок файла используется во всех файлах, предназначенных для данного программного комплекса.

Первой записью после заголовка является количество записей в антивирусной базе (целое число без знака размером 64 бит).

Каждая запись в антивирусной базе включает:

Строку в кодировке UTF16-LE – название вируса

Строку в кодировке UTF-16LE – тип файла, в которых встречается данная сигнатура (“PE” или “ZIP”)

Целое число без знака 64 бит – длина сигнатуры в байтах

Целое число без знака 64 бит – префикс сигнатуры (первые 8 байт)

Целое число без знака 64 бит – смещение начала диапазона, в котором встречается сигнатура, относительно начала файла

Целое число без знака 64 бит – смещение конца диапазона, в котором встречается сигнатура, относительно начала файла

ASCII строку длиной 64 символа – хэш сигнатуры (для сигнатур длиной 8 байт используется строка “No Hash”)

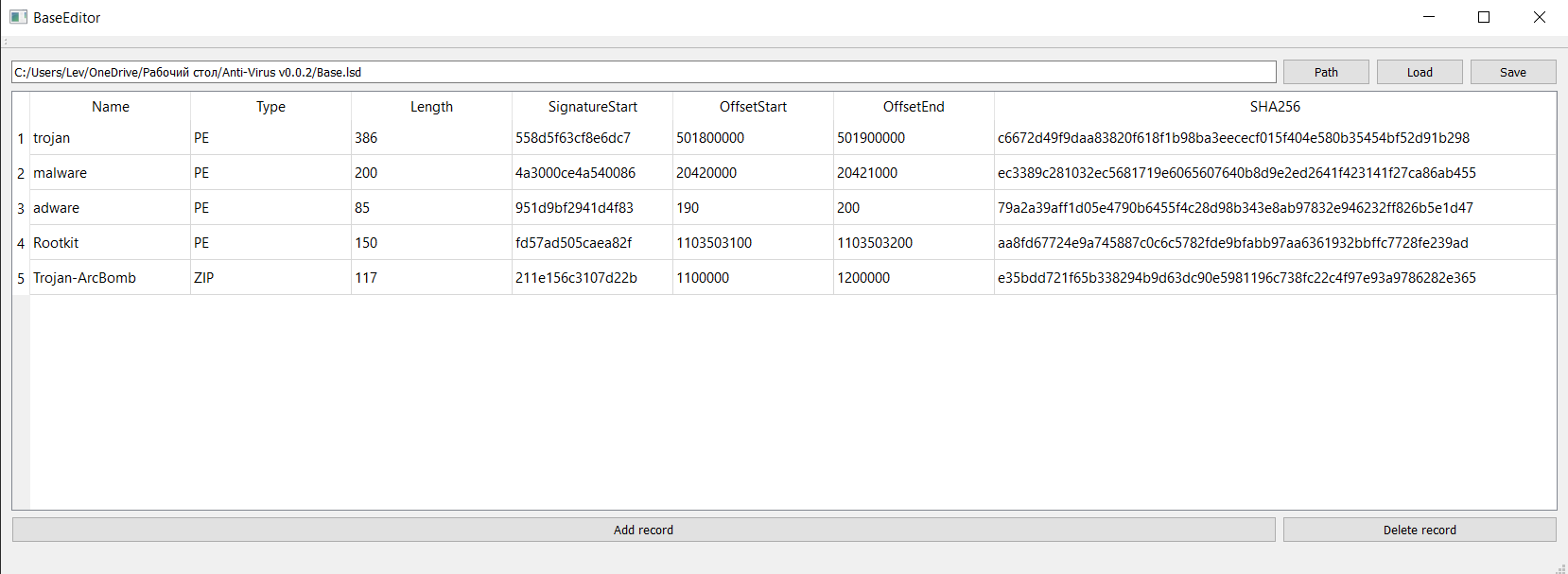


Рисунок 1 – интерфейс редактора баз

**Клиентское приложение**

Функционал:

1. Выбрать папку или файл для сканирования
2. Остановить сканирование
3. Отобразить список найденных угроз
4. Удалить найденную угрозу
5. Поместить в карантин найденную угрозу
6. Вернуть из карантина найденную угрозу
7. Запланировать проверку
8. Отменить запланированную проверку
9. Установить мониторинг папки
10. Отменить мониторинг папки
11. Отключение серверного приложения

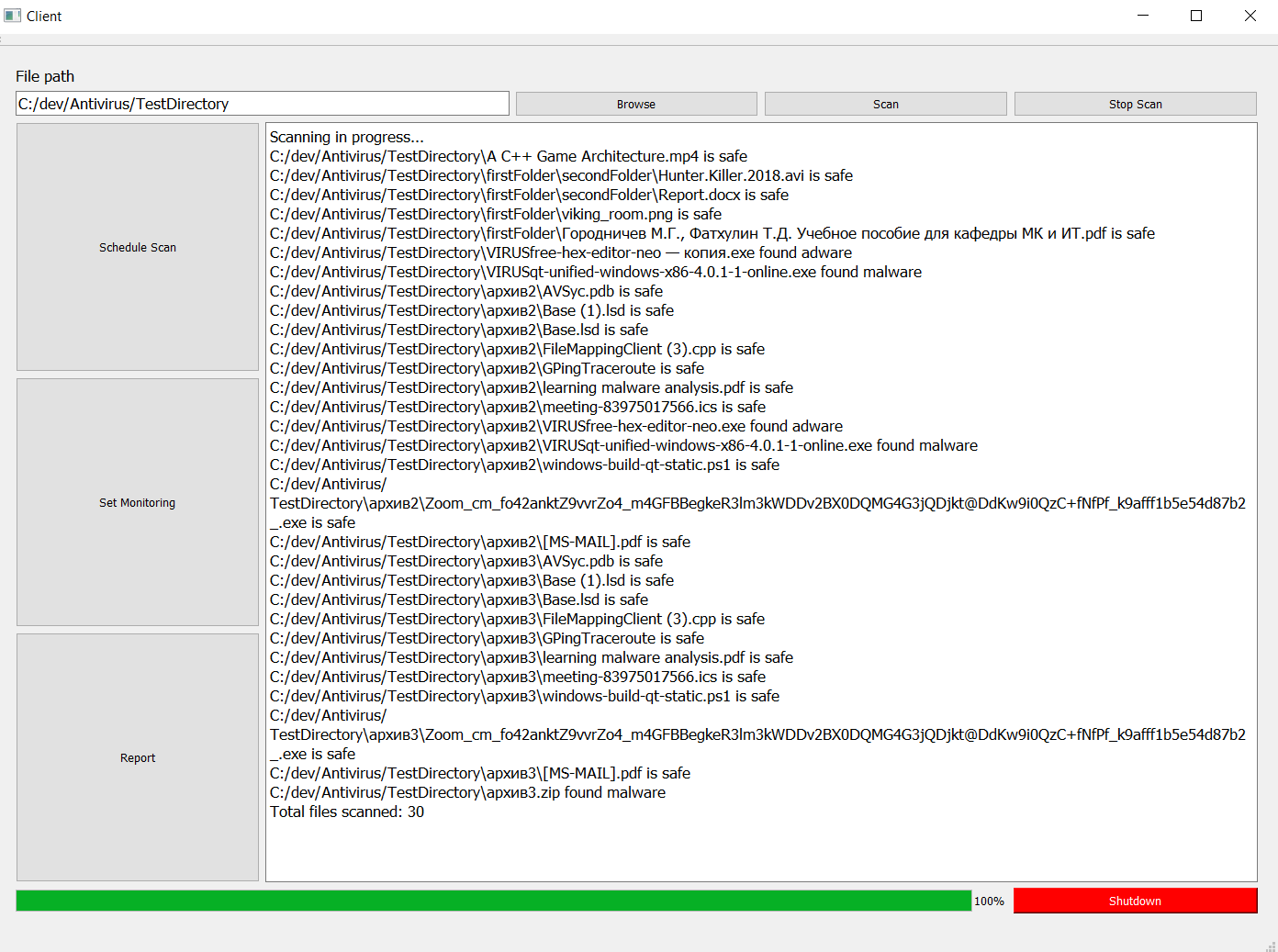


Рисунок 2 – интерфейс клиентского приложения

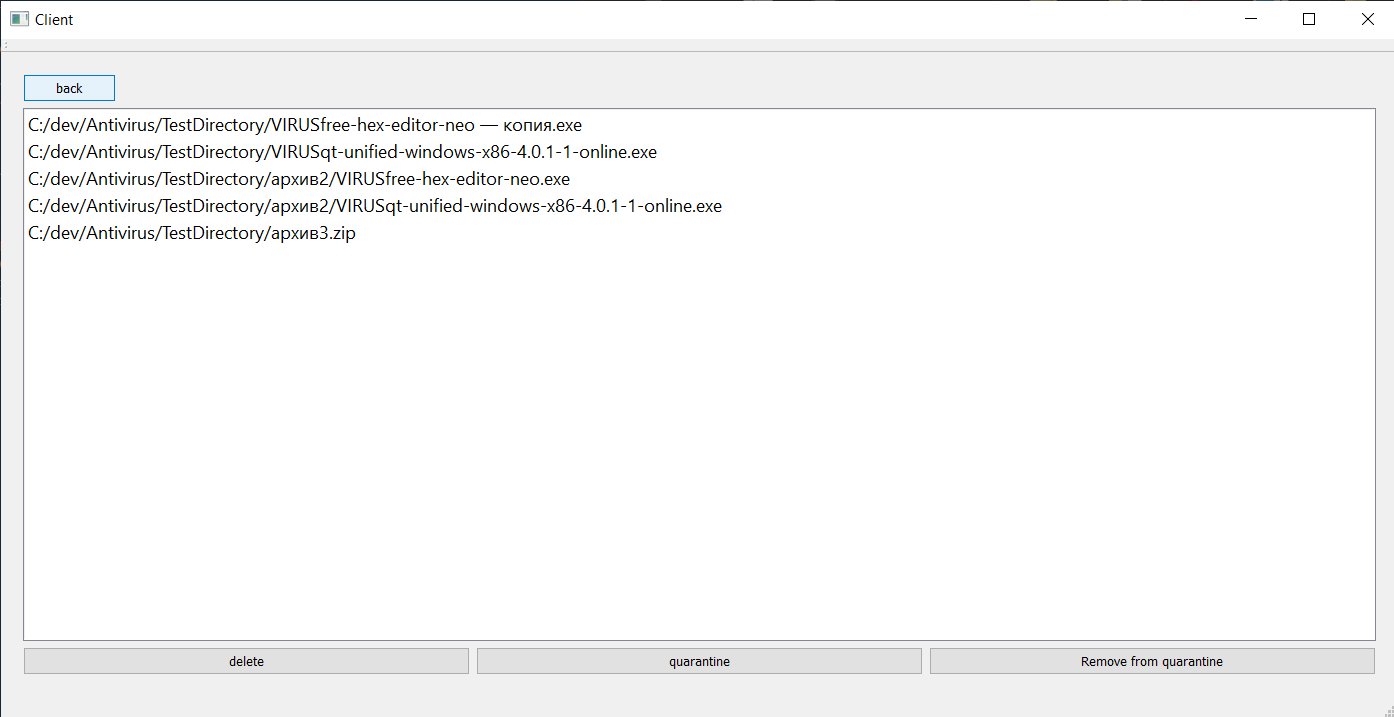


Рисунок 3 – список обнаруженных угроз

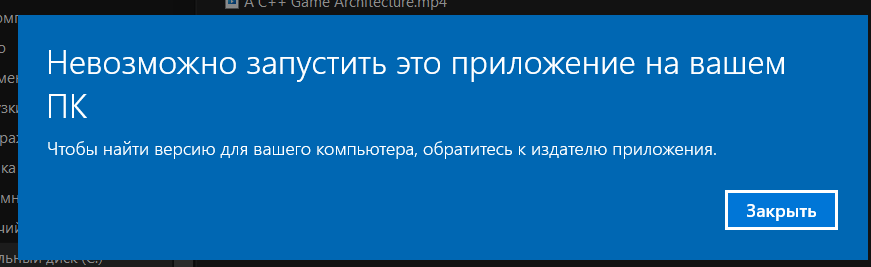


Рисунок 4 – попытка запустить PE файл после помещения в карантин

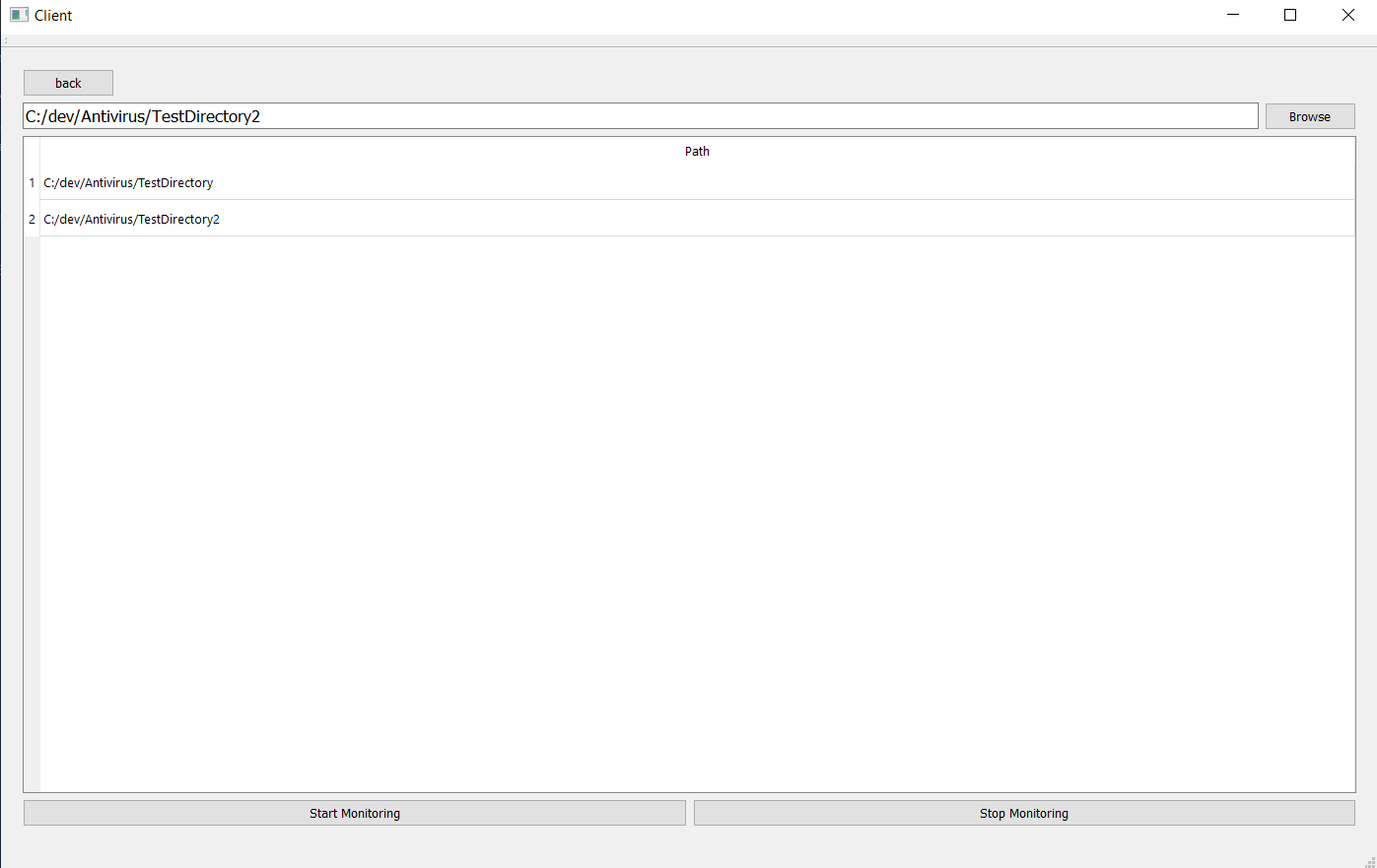


Рисунок 5 –Установка мониторинга папки

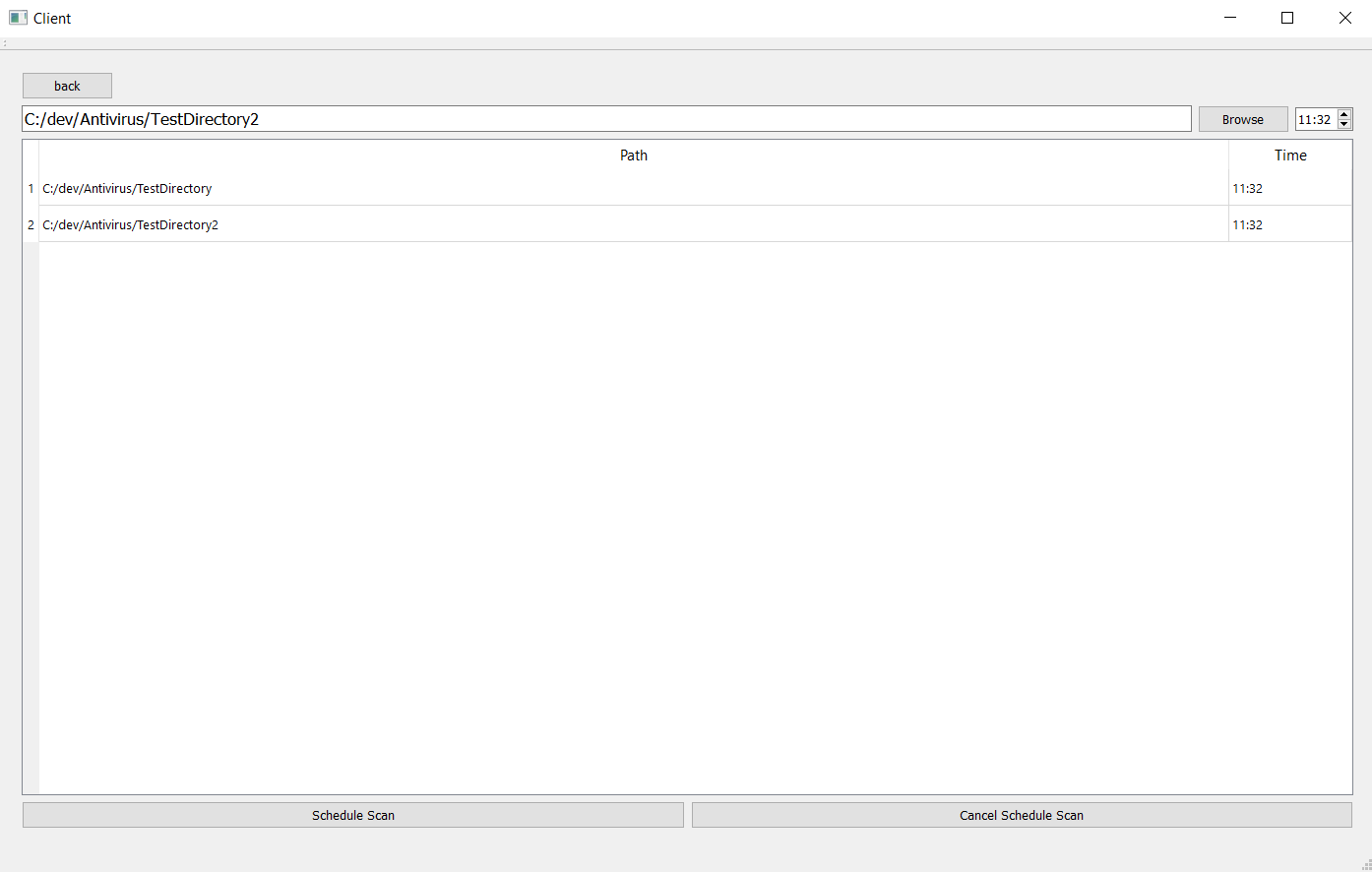


Рисунок 6 – запланировать проверку папки

**Серверное приложение**

Серверное приложение является службой Windows, которая в фоновом режиме ожидает запросов от клиента и выполняет их. Остановить данную службу можно из клиентского приложения. Также служба принимает сообщение о выключении компьютера, чтобы сохранить текущие угрозы, мониторинги и запланированные проверки в постоянную память.

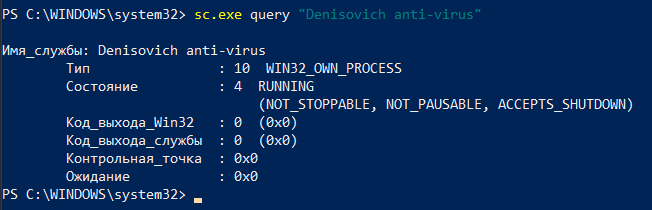


Рисунок 7 – описание службы в менеджере сервисов Windows

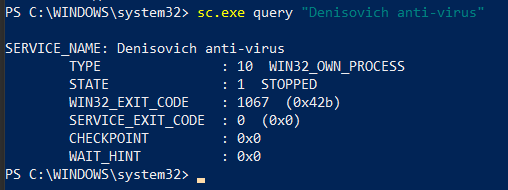


Рисунок 8 – служба остановлена после нажатия кнопки выключения из клиента

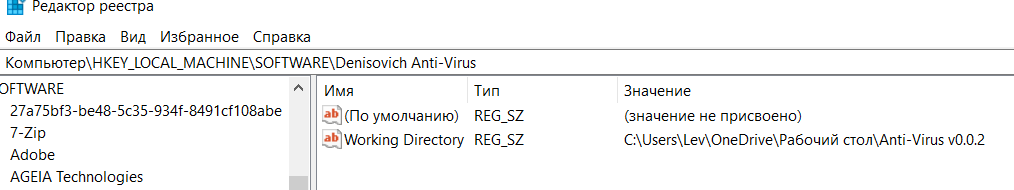


Рисунок 9 – помещение рабочего каталога в реестр для последующей корректной работы службы

Каждое сканирование производится в отдельном потоке, что позволяет проводить несколько сканирований одновременно. Мониторинг каждой папки и каждая запланированная проверка также работают в отдельном потоке.

Для того, чтобы при запуске программного комплекса возобновлять все заблокированные проверки и все установленные мониторинги, они помещаются в файл при выключении серверного приложения, которое происходит либо при нажатии пользователем соответствующей кнопки, либо при выключении компьютера.

**Исходный код**

Весь исходный код проекта доступен по ссылке:

<https://github.com/NiceNickname/SimpleAntivirus>