**Федеральное агентство связи**

**Ордена Трудового Красного Знамени**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

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

Кафедра Математической Кибернетики и Информационных Технологий

****

**Отчет по проектной работе**

по предмету «ЗИотВПО»

на тему:

«Антивирус»

Выполнил: студент группы

БВТ1802

Дворянинов П. В.

Руководитель:

Барков В. В.

Москва 2021

**Цель**

Разработка антивирусной защиты согласно плану технического задания.

**Выполнение**

Весь программный код антивируса представлен на GitHub:

<https://github.com/PaviliuS/AntiVirus>

Запуск приложения осуществляется на следующей ОС:

* ОС Windows 10 64-bit.

Межпроцессное взаимодействие происходит с помощью Pipes, используем три вида Pipes:

– hPipe – канал для обычного сканирования;

– hPipeScheduled – канал для сканирования по расписанию;

– hPipeMonitor – канал для мониторинга.

Типы данных, которые могут пересылаться между приложениями:

* INT8;
* INT16;
* INT32;
* INT64;
* UINT8;
* UINT16;
* UINT32;
* UINT64;
* PATH.

**Хранение вредоносных сигнатур в БД**

Антивирусные базы хранятся в бинарном файле. Заголовок данного файла, по плану ТЗ, представляет фамилию студента на латинице «Dvoryaninov». Данный заголовок работает с файлами, которые предназначены для данного приложения.

Каждая запись в антивирусной БД включает:

– Название вируса;

– Тип файла, в которых встречается данная сигнатура;

– Префикс сигнатуры;

– Длина сигнатуры в байтах;

– Хэш сигнатуры;

– Смещение начала диапазона, в котором встречается сигнатура, относительно начала файла;

– Смещение конца диапазона, в котором встречается сигнатура, относительно начала файла.

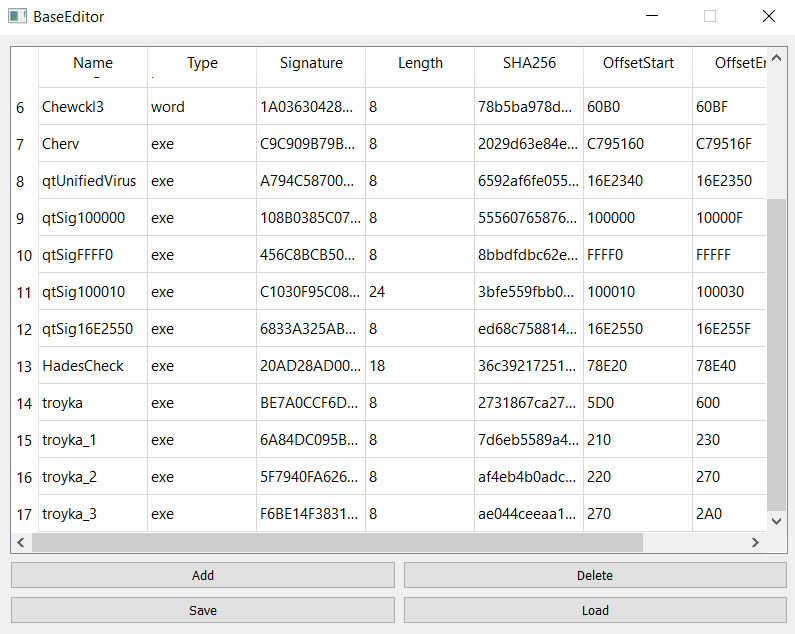


Рисунок 1 – Приложение для редактирования БД

**Клиентское приложение**

Данное клиентское приложение содержит следующий функционал:

– Выбор каталога или файла для сканирования;

– Запуск сканирования;

– Отмена сканирования;

– Запуск мониторинга;

– Отмена мониторинга;

– Запуск сканирования по расписанию;

– Отмена сканирования по расписанию;

– Установка времени.

Также приложение содержит специальные поля для вывода обнаруженных угроз и для вывода истории в журнал.

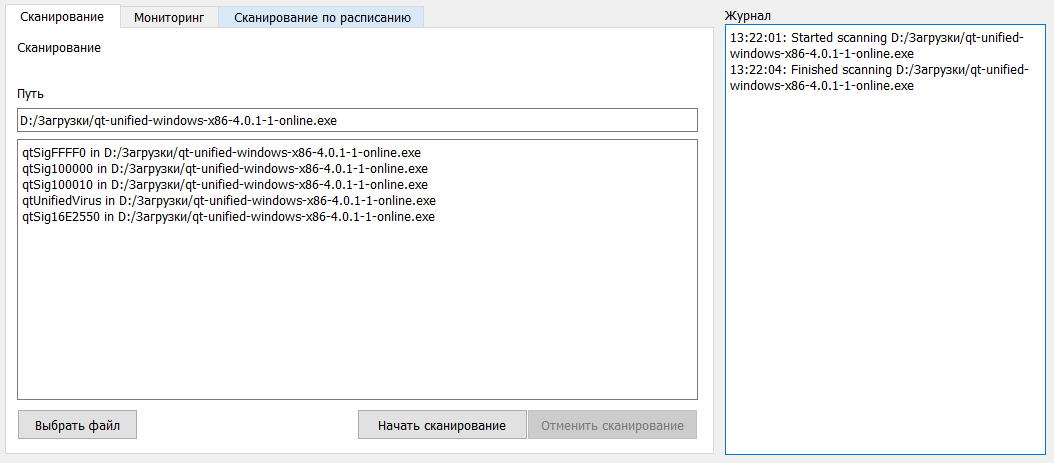


Рисунок 1 – Обычное сканирование файла

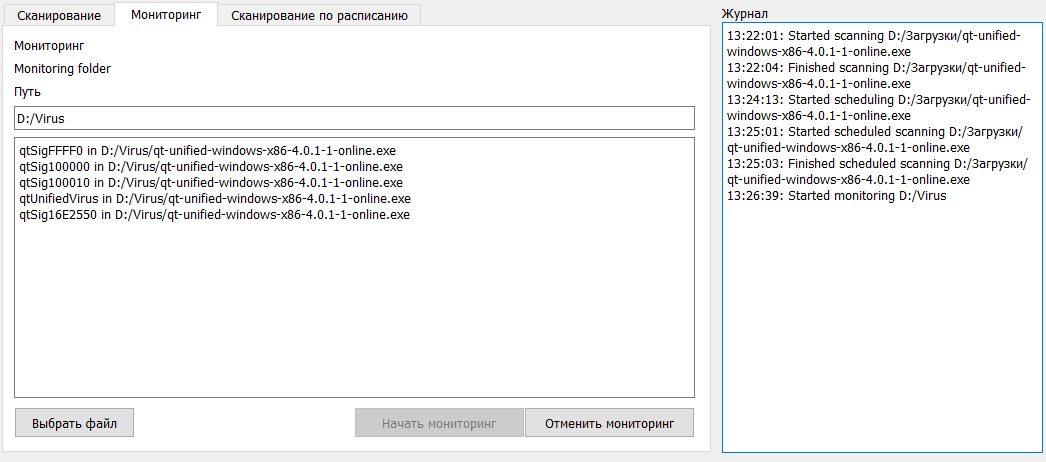


Рисунок 2 – Мониторинг каталога

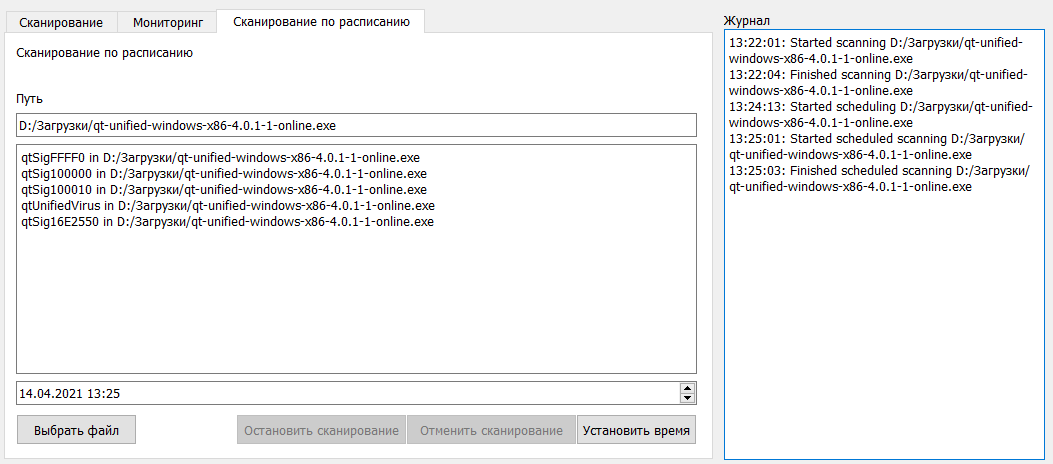


Рисунок 3 – Сканирование по расписанию

**Серверное приложение**

Серверное приложение является службой Windows, которая вызывается после запуска приложения автоматически. После запуска, данная служба работает в фоне и ожидает соответствующих запросов от клиента. Выключение данной службы происходит через «Диспетчер задач» ОС Windows.

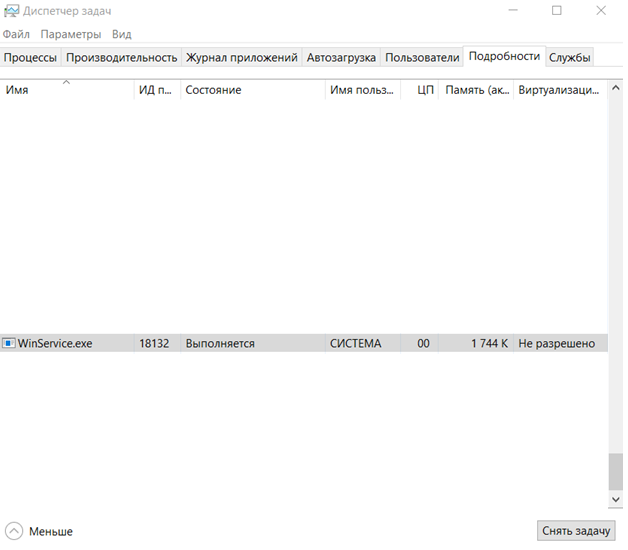


Рисунок 1 – Работа приложения в фоне

Каждое сканирование производится в отдельных потоках. Это позволяет инициализировать несколько сканирований одновременно. Клиент может запустить обычное сканирование файла, мониторинг каталога и сканирование по расписанию одновременно.

**Вывод**

Разработали антивирусную защиту согласно плану технического задания.