**Федеральное агентство связи ордена Трудового Красного Знамени федеральное государственное бюджетное общеобразовательное учреждение высшего образования «Московский технический университет связи и информатики»**

Кафедра Информационная безопасность

Отчет по Антивирусу

По дисциплине «Защита информации от вредоносного программного обеспечения»

Выполнил: студент группы БВТ1801

Клюшкин Дмитрий Алексеевич

Проверил:

Барков Вячеслав Валерьевич

Москва 2021

Содержание

[Введение 3](#_Toc67603239)

[Динамическая библиотека классов 4](#_Toc67603240)

[SearchFile 4](#_Toc67603241)

[ScanObject 4](#_Toc67603242)

# Введение

При разработке собственного антивируса, следует определиться с важными моментами как: язык разработки службы и клиентского приложения, способ общения между ними, реализация хранения антивирусной сигнатуры, представление результатов сканирования и т.д. Немалую роль играет архитектура антивирусного комплекса. Важно придерживаться проектирования с применением принципов дизайна классов (S.O.L.I.D.) и принципов организации компонентов. Это придаст коду большую читабельность и позволит избежать возникновения различных проблем.

# Динамическая библиотека классов

В проекте имеется динамическая библиотека классов AntiLib.dll. Она содержит все необходимые методы для работы сервиса. В неё входят:

* SearchFile – рекурсивный поиск PE файлов;
* ScanObject – извлечение секции .text из PE файла;
* ScanFile – поиск сигнатуры в экземпляре класса ScanObject;
* FileObserver – создание события на мониторинг директории.
* DateValue – содержит глобальные переменные для создания отчета и таймер для запуска сканирования по расписанию.
* DBManager – содержит все необходимые запросы.
* MCF и IMCF – класс для работы WCF.

## SearchFile

Статический класс, который содержит два публичных метода: SearchFileDirectory и GetTypeFile.

SearchFileDirectory принимает на вход путь до директории/файла и операцию, которую надо будет совершить над файлом, если он окажется заражен. Операция над файлом не потребуется в текущем методе, но будет передана последующим. Этот метод может завершить сканирование, если все файлы были отсканированы и все объекты для сканирования были переданы. Найденные файлы передаются в ScanObject. Данный метод работает в совокупности с GetTypeFile.

GetTypeFile принимает на вход путь до файла, считывает первый байт и если имеется начало PE файла, отправляет обратно значение для уведомления.

## ScanObject

Класс, который содержит конструктор для извлечения секции .text из PE файла. Считывает расположение .text и его размер и извлекает его в массив байтов. Используется для передачи классу ScanFile.

## ScanFile