**Техническое задание на разработку комплекса антивирусной защиты**

**Срок выполнения:**

1 апреля 2021 (автомат)

20 мая 2021

**Требования к архитектуре**

1. Комплекс антивирусной защиты должен включать следующие компоненты:
   1. Антивирусные базы.
   2. Сервис, осуществляющий проверку заданных объектов.
   3. Клиентское приложение для управления сервисом и получения результатов (UI).
   4. Приложение для редактирования содержимого антивирусных баз.
2. Общий функционал должен быть вынесен в отдельные библиотеки и использоваться компонентами комплекса совместно.
3. Все компоненты должны быть разбиты на модули.
4. Модули должны быть спроектированы с применением принципов дизайна классов (S.O.L.I.D.) и принципов организации компонентов.
5. Все компоненты должны быть построены с применением одного из архитектурных паттернов (например, Clean Architectur).
6. При необходимости разработанные модули должны поставляться с модульными тестами. (опционально)

**Антивирусные базы**

1. Антивирусные базы должны представлять собой бинарные файлы в файловой системе или базу данных (например, SQLite).
2. Файлы антивирусных баз должны начинаться со специальной последовательности байтов, которые гарантируют, что базы предназначены именно для вашего комплекса. В качестве такой последовательности следует выбрать последовательность строчных латинских символов, представляющих фамилию студента.
3. Файлы антивирусных баз должны хранить общее количество записей и информацию о каждой отдельной записи.
4. Запись антивирусной базы включает в себя:
   1. Название вредоносного объекта (строка, с предварительным указанием её длины)
   2. Сигнатуры вредоносного объекта (один из вариантов):
      1. Длина сигнатуры, префикс сигнатуры фиксированной длины (n байтов), SHA256 (или иной хэш) сигнатуры
      2. Длина сигнатуры, данные сигнатуры
   3. Смещение сигнатуры относительно начала сканируемого объекта, задаваемое в виде интервала [offsetBegin; offsetEnd].

**Сервис.**

1. Разрабатываемый сервис должен поддерживать следующие функции:
   1. Сканирование указанного файла.
   2. Сканирование указанной папки (рекурсивно).
   3. Мониторинг указанной директории и сканирование новых файлов, создаваемые в ней или копируемых/перемещаемых в неё.
   4. Сканирование по расписанию.
2. Сервис должен поддерживать сканирование следующих объектов:
   1. PE и опционально ELF-файлов
   2. ZIP архивов:
      1. Одноуровневых
      2. Вложенных.
3. Сервис должен включать в себя следующие модули:
   1. Модуль загрузки антивирусных баз – представление баз в виде TST-дерева, либо в виде RB-дерева (при условии фиксированного ключа), ключами являются данные сигнатуры.
   2. Модуль обнаружения сканируемых объектов – определяет по содержимому файла его тип и создаёт один или несколько объектов для сканирования (сегменты кода, либо содержимое для PE файлов, сегменты кода, либо содержимое для каждого PE файла в архиве, в том числе во вложенных архивах).
   3. Модуль обхода заданной директории – рекурсивно обходит все файлы в директории и уведомляет о каждом найденном файле.
   4. Модуль мониторинга директории – ожидает появления новых файлов в заданных директориях и уведомляет о новых файлах.
   5. Модуль сканирования объектов – осуществляет сканирование объектов. Ищет совпадение части сканируемого объекта с ключом (или его префиксом) из базы. При успешном поиске проверяет дополнительные условия (попадание смещения сигнатуры в диапазон, указанной в записи, совпадение хэша всей сигнатуры при использовании хэшей).

**Клиентское приложение для управления сервисом и получения результатов.**

1. Приложение должно иметь графический пользовательский интерфейс.
2. Приложение должно уметь при необходимости запускать и останавливать сервис.
3. Приложение должно уметь отправлять следующие команды сервису:
   1. Запустить сканирование папки
   2. Запустить сканирование файла
   3. Остановить сканирование
   4. Запустить мониторинг директории
   5. Остановить мониторинг директории.
   6. Запланировать проверку по расписанию
4. Приложение должно уметь принимать от сервиса результаты сканирования.
5. Приложение должно уметь показывать текущее состояние сканирования (запущено, не запущено, какой файл сканируется).
6. Приложение должно уметь показывать результаты сканирования, включающие количество найденных файлов, количество просканированных объектов, количество найденных угроз и список заражённых объектов.

**Приложение для редактирования содержимого антивирусных баз**

1. Приложение для редактирования содержимого баз должно уметь читать и записывать записи в антивирусные базы.
2. Приложение должно уметь отображать содержимое добавляемого файла. Область файла, добавляемая в качестве сигнатуры, должна выбираться путём выделения части содержимого файла.