**Функциональные требования к ПО**

1.Введение

1.1. Цель

Создать систему у которой обеспечена непрерывная выгрузка зашифрованных данных с сервера, расшифровка с помощью ключа, отправка на промежуточное хранилище в защищенном виде.

1.2. Контекст

Система будет использоваться в среде Windows для непрерывного мониторинга и обработки данных, поступающих с удаленного сервера.

2. Сбор данных

Система должна подключаться к WebSocket-серверу по адресу \_\_\_\_

Система должна принимать массив из 10 строк каждые 20 секунд.

Система должна декодировать данные в формате Base64 в бинарный вид для обработки.

3.Обработка данных

Система должна расшифровывать данные с помощью: алгоритма AES-CBC, ключа на флэш-накопителе и извлеченного IV.

Система должна обрабатывать блоки с помощью Padding для получения исходного Json-объекта.

4.Хранение данных

Система должна сохранять расшифрованные данные в защищенном формате в хранилище (База Данных PostgreSQL)

Система должна поддерживать структуру хранения данных для агрегации.

5.Мониторинг

Система должна логировать успешные операции (подключение к серверу, прием данных, расшифровка данных, подключение к базе данных)

Система должна обрабатывать ошибки (некорректные данные, ошибки при подключении к серверу и к базе данных, сбой при расшифровке данных, сбой при отправке уведомлений на почту).

Система должна отсылать уведомления на email администратору при возникновении ошибок.

6.Интерфейс

Система должна предоставлять консольный интерфейс для отображения данных из таблицы PostgreSQL

Данные должны выводиться в виде таблицы с фиксированными столбцами

Данные должны обновляться с заданной периодичностью

7.Требования к данным

Данные должны сохранятся в PostgreSQL

Пароли должны быть в зашифрованном виде

8.Требования к интеграции

Система должна интегрироваться с SMTP-сервером для отправки уведомлений

9.Требования к отказоустойчивости

Система должна переподключаться при разрыве соединения каждые 5 секунд

10.Безопасность

Система должна обеспечивать защиту от несанкционированного доступа

Ключ не должен сохранятся в открытом виде в логах

Ключ шифрования и расшифровки должен храниться на флэш-накопителе