# Проектирование кибериммунного устройства мониторинга оборудования (КУМО)

## 1 Общее описание продукта

### Назначение и применение продукта

Данный продукт используется в промышленных сферах, где используется какое-либо оборудование для производства. Решение считывает показатели всех устройств и следит за их значениями. В случае превышения пороговых значений система генерирует событие, которое может получить пользователь для дальнейшего анализа. В данном случае предполагается использовать данную систему на заводе по производству лекарств.

### 1.2 Ценности продукта

Данное решение позволяет в постоянном режиме следить за всеми показателями устройств на заводе, а в случае превышения какого-либо значения система генерирует события с соответствующими данными (время превышения, какой показатель был превышен, на какую величину, какой аппарат, что он выпускает и т.д.).

## 2 Характеристики системы

### 2.1 Активы

В данном случае активы — это всё оборудование, у которого отслеживаются показатели.

### 2.2 Ущерб

Ущерб при атаке на данную систему - утечка данных показателей оборудования, невозможность считать показатели, неработоспособность системы.

### 2.3 Возможные риски

Исходя из ущерба, можно выделить и риски - существует возможность утечки данных или вывода из строя системы или её частей.

## 3 Концепция безопасности системы

Исходя из вышеперечисленных пунктов можно сформулировать основную концепцию безопасности данной системы - никакие данные не могут быть получены неавторизованными лицами и недопустим удалённый доступ ими к системе, а также недопустим выход системы из строя.

## 4 Цели и предположения безопасности системы

### 4.1 Цели безопасности

1. Система считывает только подключенное к ней оборудование;
2. Все оборудование выдаёт только реальные показатели, которые относятся именно к нему;
3. Система сообщает о попытках взлома.

4.2 Предположения безопасности

1. Защита от неавторизованного доступа;
2. Защита от намеренного искажения показателей оборудования;
3. В случае бездействия пользователя, система выходит из его аккаунта.

## 5 Сценарии использования системы

### 5.1 Ключевые сценарии использования

1. Просмотр характеристик оборудования;
2. Изменение пороговых значений;
3. Анализ событий, созданных системой при превышении пороговых значений.

### 5.2 Негативные сценарии

1. Установление слишком маленьких или слишком больших величин пороговых значений, вследствие чего возникает слишком много событий или система их не создаёт, когда надо;
2. Удаление части оборудования из системы программных способов неавторизованным пользователем.
3. Добавление несуществующего оборудования в систему.

## 6 Архитектура системы



1. Ядро системы – обработка поступающих данных с оборудования, создание и отправка событий при превышении значений;
2. Оборудование 1, 2, …, N – само оборудование, у которого есть некоторые показатели;
3. Блок считывания данных – постоянно получает данные с оборудования, к которому он подключен, преобразовывает их в удобный вид и отправляет в ядро;
4. Блок вывода событий – получает события от ядра, преобразует их в понятный для пользователя в вид и отправляет их на ПК пользователя и администратора;
5. ПК пользователя – может получать и анализировать события, просматривать доступное оборудование и смотреть за их показателями;
6. ПК администратора – может делать всё то же, что и пользователь, а также менять пороговые значения, добавлять и удалять оборудование из системы;