РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

**Модуль централизованного мониторинга событий на рабочих станциях сотрудников объекта КИИ «Стражник»**

Автор: Подкина Ю.А

**ОГЛАВЛЕНИЕ**

**1. ОПИСАНИЕ СИСТЕМЫ**

**2. РЕАЛИЗАЦИЯ СЕРВИСА КОНТРОЛЯ ДОСТУПА**

**2.1 Вход в систему**

**2.2 Функционал Администратора доступа**

1. **ОПИСАНИЕ СИСТЕМЫ**

«Стражник» – система централизованного мониторинга событий на рабочих станциях сотрудников министерства обороны РФ (МО) и оборонных предприятий. Система позволяет в режиме реального времени выявлять возможные угрозы информационной безопасности (ИБ), оперативно на них реагировать, отправлять уведомления службе безопасности, соблюдать условия мандатного доступа к данным пользователей.

Система «Стражник» состоит из набора сервисов, взаимодействующих между собой по протоколу удалённого вызова процедур – gRPC, программному интерфейсу приложений – API, протоколу обмена сообщений – WebSocket.

В состав системы входят следующие сервисы:

1. сервис контроля доступа;
2. сервис протоколов безопасности;
3. сервис логирования;
4. сервис сообщений;
5. клиентское приложение для ПК;
6. клиентское приложение для мобильных устройств.

Пользователями системы являются предприятия выполняющие государственный оборонный заказ (ГОЗ) и Министерство обороны.

Основная цель системы состоит в предотвращении утечки данных о выполнении гособоронзаказа. Предприятия выполняющие ГОЗ должны иметь возможность загрузить в систему выпускаемую ими номенклатуру продукции, указать степень выполнения ГОЗ по каждой группе номенклатуры. Служащие МО должны иметь возможность получить сводные данные о степени выполнения ГОЗ по предприятиям и видам заказанной у предприятий продукции.

С целью обеспечения оперативной работы службы ИБ, необходимо реализовать клиентское приложение для мобильных устройств, которое позволит сотруднику службы ИБ получать информацию о несанкционированных действиях пользователей системы и сообщения от заблокированных пользователей.

1. **РЕАЛИЗАЦИЯ СЕРВИСА КОНТРОЛЯ ДОСТУПА**

Основой системы «Стражник» является контроль доступа пользователей к данным гособоронзаказа. Все пользователи системы разделены на четыре основные группы:

1. администраторы доступа на предприятиях и в МО;
2. руководители производственных отделов предприятий;
3. служащие МО отвечающие за контроль выполнения ГОЗ;
4. пользователи службы ИБ.

В качестве этой группы пользователей выступают сотрудники отделов ИБ оборонных предприятий и служащие отделов ИБ Министерства обороны.

Управление ролевой моделью системы и доступом пользователей к системе осуществляет «Сервис контроля доступа». Он обрабатывает запросы на авторизацию пользователей в системе, через него происходит добавление новых пользователей в систему.

* 1. **Вход в систему**

Добавление новых пользователей в систему осуществляют Администраторы доступа. Администраторами доступа являются сотрудники предприятий с соответствующими правами и служащие МО обладающие данной ролью.

После запуска системы – клиентского приложения для ПК, пользователя встречает окно входа в систему (Рис. 1). Пользователь с ролью «Администратор доступа» должен выбрать тип пользователя «Администратор доступа» из выпадающего списка, ввести логин, пароль и секретное слово. После ввода необходимых данных пользователь авторизуется в системе нажимая на кнопку «Войти в систему». В случае выхода из системы, процедура авторизации проходится заново.

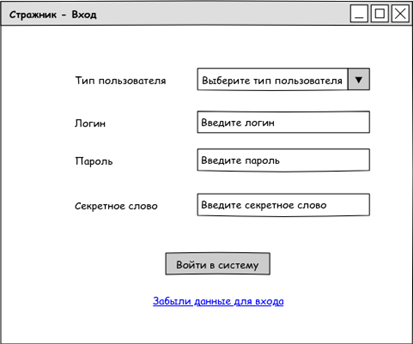


Рис. 1. Прототип окна входа в систему

**2.2 Функционал Администратора доступа**

После успешного входа в систему «Администратор доступа» перенаправляется в окно «Управление доступом» (Рис. 2). В открывшемся окне должна быть возможность указать данные нового пользователя системы: ФИО, пол, должность, загрузить фотографию.

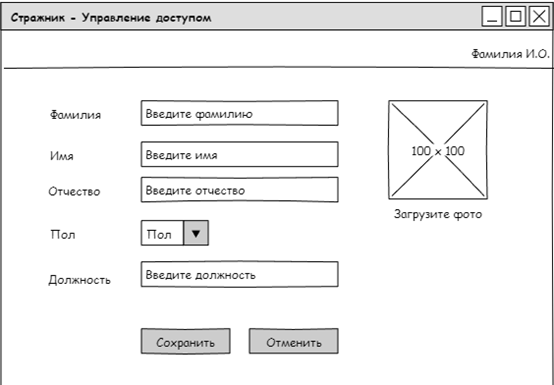


Рис. 2. Прототип окна управление доступом

После заполнения необходимых данных «Администратор доступа» может сохранить введенные данные нажав на кнопку «Сохранить». После чего, данные записываются в базу данных, и направляются на верификацию пользователю с ролью «Пользователь службы ИБ». Все введённые данные в полях и фотография очищаются. Система уведомляет пользователя, о том, что данные сохранены. Пользователь остаётся в этом же окне.

Если при добавлении нового пользователя, «Администратор доступа» нажал на кнопку «Отмена», все введённые данные в полях и фотография очищаются. Система уведомляет пользователя, о том, что данные очищены. Пользователь остаётся в этом же окне.