

## **СЕССИЯ 4**

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

«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.

В состав системы «Стражник» входят инструменты мониторинга, обработки и аудита событий на персональных компьютерах (ПК) пользователей, средства визуализации данных для службы ИБ, механизмы оповещения службы ИБ о событиях, нарушающих протоколы безопасности.

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:

- сервис контроля доступа;
- сервис протоколов безопасности;
- сервис логирования;
- сервис сообщений;
- клиентское приложение для ПК;
- 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.

Система должна обладать режимом мандатного доступа к данным, т.е. каждая из имеющихся групп пользователей системы получает возможность просматривать определённый вид данных в соответствии с протоколами безопасности. При попытке несанкционированного доступа к данным, со стороны пользователя, система должна осуществлять блокировку действий пользователя, с уведомлением службы безопасности предприятия или МО. Заблокированный пользователь должен иметь возможность связаться с представителем службы ИБ через чат клиентского приложения для ПК.

Для обеспечения наибольшего уровня безопасности, все действия пользователей системы, должны логироваться в режиме реального времени, данные о действиях всех пользователей направляются в службы безопасности предприятий и МО.

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.

**В рамках Сессии 4 вам необходимо начать разработку модуля «Стражника» - сервис контроля доступа.**

## **ПРОЕКТИРОВАНИЕ, РАЗРАБОТКА БАЗ ДАННЫХ И ИМПОРТ**

На основе описания предметной области, текста задания, имеющихся макетов, исходных данных вам необходимо разработать базу данных в выбранной СУБД. Разработанная в рамках четвертой сессии база данных будет использоваться и расширяться в следующих сессиях. На протяжении всей разработки модуля «Стражник» необходимо использовать данную БД.

Также необходимо импортировать данные из предоставленных файлов в папке “import”. Если каких-либо данных не предоставлено, заполните базу данных тестовыми данными (не менее 3 записей).

## **ПРОЕКТИРОВАНИЕ НА ЯЗЫКЕ UML**

Для реализации системы «Стражник» вам необходимо провести логическое моделирование архитектуры создаваемых сервисов, используя «Контейнер-диаграмму» (Container). Для этого проанализируйте описание предметной области, выделите необходимые технологические решения и способы их взаимодействия (контейнеры и их функции, протоколы обмена данными между контейнерами). Обратите внимание, что выделенные вами контейнеры и протоколы их взаимодействия, могут отличаться от итоговой реализации системы.

Разработанную диаграмму сохраните в формате PDF используя шаблон наименования – «Контейнер\_диаграмма\_номер\_вашего\_рабочего\_места».

Разработайте диаграмму вариантов использования по системе «Стражник».

Разработанные вами диаграммы должны быть размещены в системе контроля версий, согласно общим требованиям представления результатов работы.

## **РЕАЛИЗАЦИЯ СЕРВИСА КОНТРОЛЯ ДОСТУПА**

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

- администраторы доступа на предприятиях и в МО;
- руководители производственных отделов предприятий;
- служащие МО отвечающие за контроль выполнения ГОЗ;
- 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.

### **Функционал Администратора доступа**

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

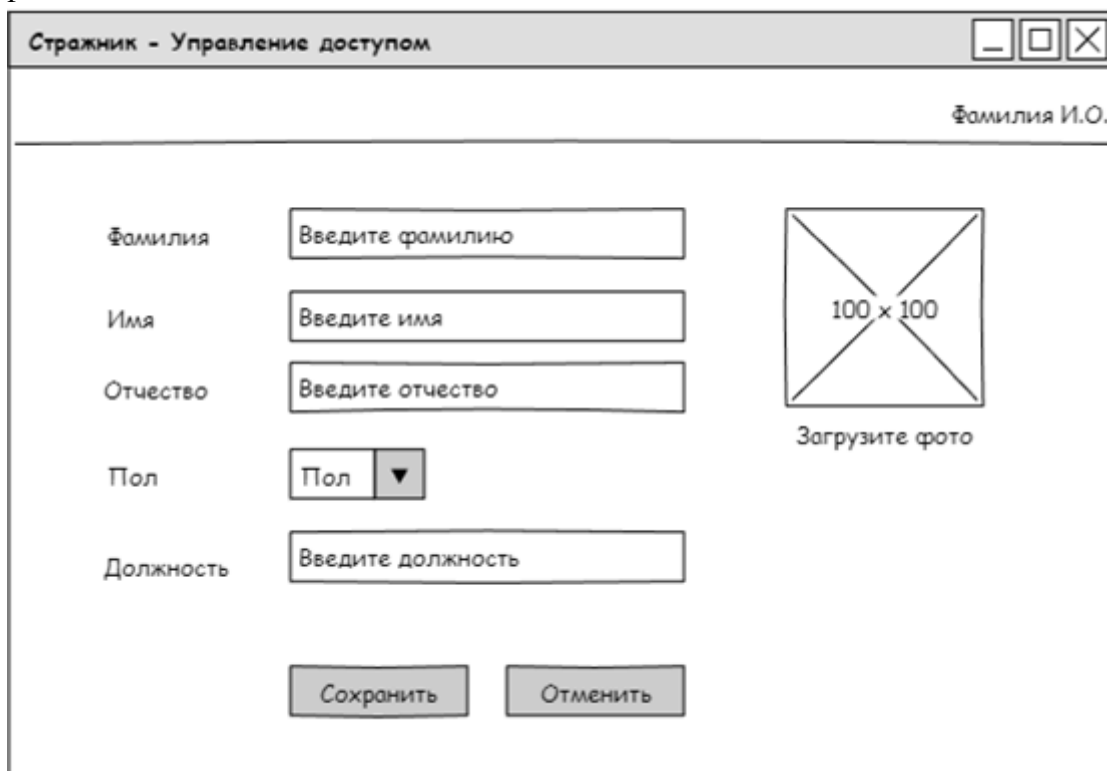
системе нажимая на кнопку «Войти в систему». В случае выхода из системы, процедура авторизации проходит заново.

После успешной авторизации в каждом окне системы отображается ФИО авторизованного пользователя в формате «Фамилия И.О.»

Рис. 1. Прототип окна входа в систему

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.



Страхник - Управление доступом

Фамилия И.О.

Фамилия

Имя

Отчество

Пол  ▼

Должность

100 x 100

Загрузите фото

Рис. 2. Прототип окна управление доступом

После заполнения необходимых данных «Администратор доступа» может сохранить введённые 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.

При двукратном нажатии на кнопку «Сохранить» и/или «Отправить» с незаполненными данными нового пользователя, происходит блокировка окна на 5 минут. Система уведомляет пользователя, о том, что окно заблокировано. При блокировке окна, поля для ввода и кнопки должны быть неактивными. Если во время блокировки «Администратор доступа» закроет приложение и повторит авторизацию, блокировка окна должна сохраняться. Общее время блокировки окна остаётся неизменным - 5 минут с момента начала блокировки.