СЕССИЯ 5

Модуль сервиса протоколов безопасности

ПРОЕКТИРОВАНИЕ НА ЯЗЫКЕ UML

В процессе разработки системы «Стражник» вам необходимо произвести декомпозицию ранее выделенных контейнер в контейнер-диаграмме. Для этого разработайте Диаграмму компонентов (Component Diagram), описывающую структурные и функциональные компоненты внутри контейнеров. Определение компонентов должно строится на описании предметной области, функций сервиса контроля доступа и функционала Администратора доступа.

Обратите внимание, что выделенные вами компоненты и их взаимосвязи, могут отличаться от итоговой реализации системы.

Разработанную диаграмму сохраните в формате PDF используя шаблон наименования – «Компонент_диаграмма_номер_вашего_рабочего_ места». Разработанная вами диаграмма должна быть размещена в системе контроля версий, согласно общим требованиям представления результатов работы.

РЕАЛИЗАЦИЯ СЕРВИСА ПРОТОКОЛОВ БЕЗОПАСНОСТИ

Протоколы безопасности являются набором правил, согласно которым, пользователи системы получают доступ к данных гособоронзаказа. Каждая группа пользователей системы обладает своим протоколом безопасности – мандатом доступа. Система должна отслеживать соблюдение мандатов доступа пользователями, в случаи их нарушения, оповещать службу ИБ предприятия или МО.

Управление мандатами доступа осуществляем сервис протокола безопасности. Группой пользователей, отвечающих за работу сервиса является сотрудники отделов ИБ оборонных предприятий и служащие отделов ИБ Министерства обороны.

Функционал Пользователей службы ИБ

Верификацию новых пользователей в системе, назначение мандатов доступа, мониторинг ИБ, аудит событий на ПК осуществляют «Пользователи службы ИБ».

Для получения доступа к системе, пользователи службы ИБ должны пройти процедуру входа в систему (Рис. 1). Пользователь с ролью «Пользователи службы ИБ» должен выбрать тип пользователя «Служба ИБ» 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.

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

Авторизованный пользователь службы ИБ перенаправляется в окно «Управление безопасностью» (Рис. 3). В окне пользователю доступны пять вкладок:

- Верификация;
- Мандаты доступа;

После входа в систему, пользователь службы ИБ автоматически перенаправляется во вкладку «Верификация». Активная вкладка выделяется цветом.

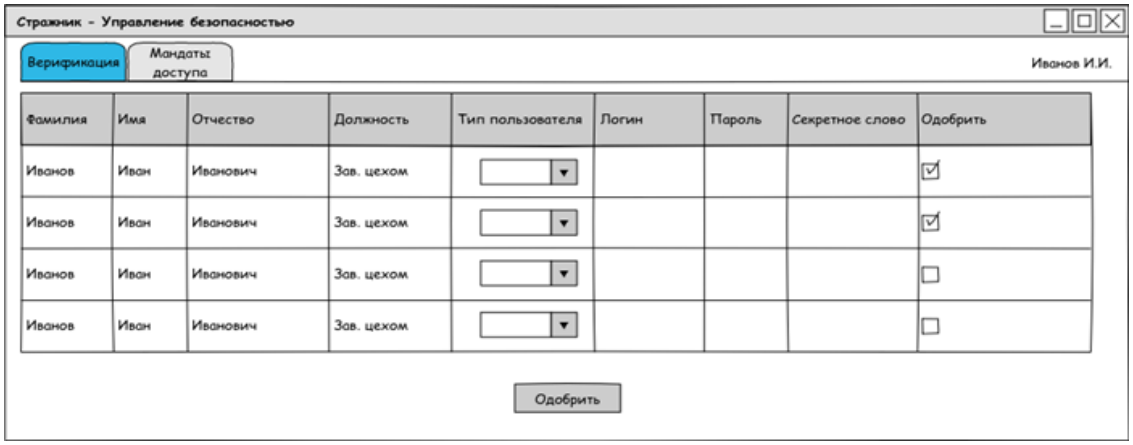

Рис. 3. Прототип окна управление безопасностью. Вкладка «Верификация»

Находясь во вкладке «Верификация» пользователь службы ИБ должен иметь возможность задать тип пользователя, логин, пароль, секретное слово и одобрить нового пользователя. ФИО и должность не редактируются. После заполнения всех полей, пользователь службы ИБ может сохранить данные нажав на кнопку «Одобрить». Все данные сохраняются в базу данных.

После сохранения, таблица с данными пользователей должна обновляться, в ней остаются только пользователи ожидающие верификации. Данные о верифицированных пользователях должны отобразиться во вкладке «Мандаты доступа».

Во вкладке «Мандаты доступа» пользователь службы ИБ должен иметь возможность назначить уровни доступа к данным для верифицированных пользователей (Рис. 4). Мандаты доступа имеют следующие уровни:

- Добавление данных;
- Просмотр данных;
- Формирование отчётов.

Новому верифицированному пользователю можно назначить мандаты доступа в любом сочетании, в зависимости от специфики его роли в системе. После назначения

мандатов доступа, пользователь службы ИБ может сохранить изменения, нажав на кнопку «Применить». Изменения сохраняются в базе данных.

Рис. 4. Прототип окна управление безопасностью. Вкладка «Мандаты доступа»

После сохранения, таблица с данными мандатов доступа должна обновляться, в ней остаются только пользователи ожидающие назначения мандатов доступа.

ТЕСТИРОВАНИЕ

Реализуйте 10 unit-тестов на основе технологии TDD для библиотеки, функционал которой описан ранее. Важно, чтобы тестовые данные предусматривали различные ситуации. Например, недостаточное время в промежутках между ранее созданными консультациями, либо в начале рабочего дня, либо в конце рабочего дня; различная длительность консультация и т.д.