# Сессия 2

**Модуль по организации контроля физического доступа к значимому объекту “ХранительПРО”**

# Терминал сотрудника общего отдела

Реализуйте терминал сотрудника общего отдела для работы с заявками, самостоятельно спроектировав графический интерфейс пользователя (ГИП).

Функционал сотрудника общего отдела:

1. авторизация по коду сотрудника (заранее определен в БД как тестовые данные);
2. просмотр списка заявок по всем данным, представленным в макетах (рисунок 3, рисунок 4);
3. фильтрация заявок по типу, подразделениям, статусу;
4. заявки, которые отклонены, должны быть раскрашены красным цветом;
5. формальная проверка заявки в отдельном модальном окне с возможностью указания даты и времени посещения, редактирования и изменения статуса заявки.

Формальная проверка выполняется системой и сотрудником общего отдела:

1. система проверяет введенные данные на отсутствие в “черном списке” посетителей и выводит сообщение с информацией об отсутствии или наличии записи в “черном списке” сразу при открытии окна с подробной информацией по заявке сотрудником общего отдела для формальной проверки (открытие модального окна для формальной проверки по заявке инициирует проверку по “черному списку”);
2. если система выдала сообщение о наличии записи по заявителю на посещение в “черном списке”, то статус заявки автоматически меняется на “Отклонена” и всем заявителям направляется сообщение “Заявка на посещение объекта КИИ отклонена в связи с нарушением [Федерального закона от 26.07.2017 № 187-ФЗ](http://ivo.garant.ru/#/document/71730198/paragraph/1:0) «О безопасности критической информационной инфраструктуры Российской Федерации»;
3. сотрудник общего отдела не может изменить решение системы об отклонении заявки в ручном режиме, то есть сотрудник при открытии окна формальной проверки не может редактировать данные по заявке, в интерфейсе все данные по заявке доступны только для просмотра, изменение статуса невозможно;
4. если система выдала сообщение об отсутствии записи в “черном списке”, сотрудник общего отдела проверяет данные на правильность заполнения, устанавливает дату и время посещения, меняет статус на “Одобрена”, и всем заявителям направляется сообщение “Заявка на посещение объекта КИИ одобрена, дата посещения: ХХ.ХХ.ХХХХ, время посещения: ХХ.ХХ;
5. если сотрудник обнаружил недостоверные данные в заявке, например номер паспорта 11111111 и прочее, сотрудник указывает статус заявки “Отклонена” и всем заявителям направляется сообщение “Заявка на посещение объекта КИИ отклонена в связи с нарушением [Федерального закона от 26.07.2017 № 194-ФЗ](http://ivo.garant.ru/#/document/71730222/paragraph/1:0) «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" по причине указания заявителем заведомо недостоверных данных”;
6. если сотрудник обнаружил отсутствие прикрепленных файлов, расхождение количества прикрепленных файлов или низкое качество прикрепленных файла(-ов), то указывается статус заявки “Отклонена” и всем заявителям направляется сообщение “Заявка на посещение объекта КИИ отклонена в связи с нарушением [Федерального закона от 26.07.2017 № 194-ФЗ](http://ivo.garant.ru/#/document/71730222/paragraph/1:0) «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" по причине указания заявителем заведомо недостоверных данных”.

“Черный список” - это данные по лицам, ранее посещавшим объект и допустившим нарушения по правилам посещения объекта КИИ. Порядок ручного формирования списка будет реализован в терминале сотрудника подразделения. Система автоматически добавляет пользователя в “черный список”, если дважды была отклонена заявка по причине указания заявителем заведомо недостоверных данных.

***Настольное приложение ХранительПро загружено в репозиторий Desktop\_Hranitel, ветка GeneralSecurity***

# Терминал сотрудника охраны

Реализуйте терминал сотрудника охраны для управления посещениями, самостоятельно спроектировав графический интерфейс пользователя (ГИП).

Функционал сотрудника охраны:

1. авторизация по коду сотрудника (заранее определен в БД как тестовые данные);
2. просмотр списка одобренных заявок по всем данным, представленным в макетах (рисунок 3, рисунок 4);
3. фильтрация заявок по дате, типу, подразделениям;
4. поиск заявки по фамилии, имени и отчеству или номеру паспорта(при групповом посещении достаточно найти одного заявителя);
5. работа с заявкой в отдельном модальном окне с возможностью указания разрешения на доступ на территорию;
6. работа с заявкой в отдельном модальном окне с возможностью указания времени убытия посетителя/посетителей.

Для разрешения на доступ в интерфейсе сотрудника охраны реализуйте элемент управления, по нажатию на который система дает сигнал о разрешении на проход (в рамках чемпионата - системный звук), открывает турникет (в рамках чемпионата - отправка сообщения на сервер об открытии турникета) и фиксирует время начала посещения в базе данных.

***Настольное приложение ХранительПро загружено в репозиторий Desktop\_Hranitel, ветка GeneralSecurity***

**ДИАГРАММА ДЕЯТЕЛЬНОСТИ**

Разработайте диаграмму деятельности добавления посетителя в «черный список».

**DATA DICTIONARY**

Разработайте словарь данных – набор информации, описывающий, какой тип данных хранится в базе данных, их формат, структуру и способы использования данных. Обратите внимание на соответствие вашей базы данных и словаря данных. Используйте подходящие типы данных, ограничения и форматы. Отразите в документе ограничения, определенные в таблицах, включая первичные ключи, отношения внешнего ключа с другими таблицами и ненулевые ограничения. Не забудьте сделать необходимые пояснения и комментарии к неоднозначным полям.

Проверка словаря данных будет выполнена по итогам работы сессий 1-4.

**ПРОЕКТИРОВАНИЕ WIREFRAME**

Разработайте  wireframe для мобильного клиента. Мобильное приложение предназначено для сотрудника охраны.

Функционал сотрудника охраны:

1. авторизация по коду сотрудника (заранее определен в БД как тестовые данные);
2. просмотр списка одобренных заявок по датам, подразделениям и типам;
3. фильтрация заявок по дате, типу, подразделениям;
4. поиск заявки по QR-коду;
5. работа с найденной заявкой в отдельном окне с возможностью указания разрешения на доступ на территорию;
6. работа с заявкой в отдельном окне с возможностью указания времени убытия посетителя/посетителей.

Важно, чтобы в wireframe была отражена логика переходов по окнам (описание, указатели, стрелки или др.).

Ваша задача в сессии 2 – только проектирование wireframe мобильного приложения.

Результат проектирования предоставьте на проверку в любом формате.

***Модуль проектирования для приложения ХранительПро загружен в репозиторий Designing\_Hranitel***