

Функциональные требования:

Идентификация:

- Система выполняет запись логина, который ввёл пользователь(email, телефон), в БД
- Гарантия отсутствия дубликатов идентификационных данных
- Должен приходить отклик от системы в случае либо некорректного ввода, либо использования уже существующего логина
- Возможность для пользователя в изменении идентификатора
- Проверка актуальности идентификатора(существует ли такой аккаунт или удалён)
- Обеспечение хранения истории изменений идентификационных данных

Аутентификация:

- Обеспечение системой записи пароля в базу данных
- Создание возможности для смены пароля
- Хранение истории паролей
- Автоматическая подстановка пароля в поле в случае повторного входа
- Сессия работы системы, пока пользователь находится на сайте, длится до выхода пользователя из сервиса, либо до входа на него
- В случае первичной регистрации пользователя выдача отклика о её успехе
- В случае успешного входа пользователя на ресурс выдача отклика об этом

Идентификация и авторизация(общее):

- Обеспечение уникальной связки(логин/пароль)

Авторизация:

- Выдача сообщения об успехе аутентификации
- Сервер предоставляет Access-token с правами доступа на ресурс при успешной регистрации
- Выдача Refresh-token для продления Access-token при успешной регистрации
- Выдача связки Access-token и Refresh-token при каждом входе пользователя на ресурс
- Автоматическое присвоение роли пользователю с учётом выданных ранее прав
- Контроль прав в ходе взаимодействия пользователя с каждым ресурсом платформы
- Сервер отзывает права пользователя в случае удаления аккаунта или при замеченном факте несанкционированных действий на ресурсах

Нефункциональные требования:

Идентификация:

- Шифрование идентификационных данных
- Возможность в создании нескольких логинов разными пользователями одновременно
- Защита от сбоев в случае высокой нагрузки на сервис
- Высокая скорость восстановления от сбоев
- Часто используемые данные кешируются
- Производится помощь пользователю в случае несоответствия корректности ввода идентификатора
- Выдача кодов ответов в случае успешного или неуспешного ввода

- Адаптивность интерфейса к различным устройствам

Аутентификация:

- Использование протокола TLS для передачи данных
- Шифрование пароля
- Анализ надёжности используемого криптографического метода защиты
- Время отклика не более 3-х секунд
- Обеспечение возможности ввода паролей несколькими пользователями одновременно
- Блокировка пользователя при подозрительной активности в виде нескольких неудачных попыток ввода пароля
- Кеширование данных
- Помощь пользователю при вводе пароля(использованы: нижний и верхний регистры латиницы, цифры, особые знаки)
- Защита от сбоев системы
- Быстрое восстановление от сбоев
- Выдача кодов ответов в случае успешного или неуспешного ввода
- Адаптивность интерфейса к различным устройствам

Авторизация:

- Шифрование токенов при передаче пользователю
- Анализ надёжности используемого метода шифрования
- Разграничение выдаваемых ролей
- Высокая скорость выдачи или изменения прав
- Возможности одновременной выдачи ролей нескольким пользователям
- Защита от сбоев системы
- Быстрое восстановление от сбоев