Лабораторная работа№8

РАЗРАБОТКА ТЕХНИЧЕСКОГО ЗАДАНИЯ НА СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ

Система авторизации пользователей

Структура документа технического задания на разработку

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

Задание разрабатывается на систему авторизации.

2 ОБЩИЕ СВЕДЕНИЯ

2.1 Полное наименование: Автоматизированная система для авторизации в разных приложениях.

2.2 Сокращенное наименование: АС Мандарик.

2.3 Заказчик: Государственное объединение «Белорусская железная дорога», 220030, г. Минск, ул. Ленина, 17;

2.4 Выполнение работ по этапам и стадиям работ, оформление и предъявление Заказчику их результатов осуществляется Исполнителем согласно требованиям данного технического задания.

3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ

3.1 Назначение Ас Мандрик

АС Мандрик предназначена для разработки и хранения в электронном виде информации необходимой для авторизации в системе.

Назначение АС Мандрик :

* Защита данных и функциональности приложений от несанкционированного доступа;
* Хранение информации необходимой для осуществления авторизации в соответствующем приложении;

3.2 Цели создания :

* автоматизация заполнения и унификация данных в соответствующей документации;
* внесение изменений в ранее веденные данные;
* формирование аргументированных замечаний со стороны согласующих и утверждающих лиц при согласовании и утверждении;
* хранение в электронном виде личной информации пользователей;
* защита конфиденциальных данных пользователей от несанкционированного доступа.
* повышение безопасности приложения и снижение риска утечки информации.
* возможность персонализации функционала приложения для разных пользователей.
* создание механизма аутентификации и авторизации, позволяющего проверять подлинность пользователей.
* удобство и быстрота доступа к информации и функциональности приложения.
* снижение риска хакерских атак и улучшение защиты приложения.
* удобство делегирования доступа к приложению разным пользователям или группам.

4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ

## 4.1 Общая характеристика объекта АС Мандрик

Система авторизации - это механизм, который позволяет проверить и подтвердить идентификационные данные пользователя для предоставления доступа к конкретным ресурсам или функциям системы. Характеристики системы авторизации могут включать в себя:

1. Безопасность: система должна обеспечивать высокий уровень защиты от несанкционированного доступа.
2. Гибкость: система должна быть настроена под конкретные потребности и права пользователя.
3. Простота использования: система должна быть удобной для пользователя, чтобы он мог быстро и легко получить доступ к ресурсам.
4. Масштабируемость: система должна быть способной масштабироваться в соответствии с растущей нагрузкой и числом пользователей.
5. Мониторинг и аудит: система должна вести журналы и аудиты для отслеживания и контроля действий пользователей и возможных нарушений безопасности.
6. Интеграция: система должна быть способной интегрироваться с другими приложениями и сервисами.
7. Поддержка разных методов аутентификации: система должна поддерживать различные методы аутентификации, такие как пароли, ключи, биометрические данные и т.д.
8. Автоматическое управление доступом: система должна предоставлять возможность автоматического управления доступом, чтобы права пользователя могли изменяться в зависимости от контекста использования.

## 4.2 Существующая система авторизации

5 ТРЕБОВАНИЯ К СИСТЕМЕ

5.1 Требования к структуре

5.1.1 Структура и содержание основных разделов

Структура и содержание основных разделов АС Мандрик устанавливается согласно требованиям ГОСТ 59383 2021.

5.1.2 Для реализации функций АС Мандрик предусматриваются следующие функциональные подсистемы:

1. Нормативно-справочная информация.
2. Информация о разработчиках.
3. Разработки и корректировки входных данных.
4. Согласование и утверждение созданной платформы авторизации.
5. Формирования выходных форм.

5.2 Требования к процедурам доступа к системе

1. Вход в систему должен быть обязателен для всех пользователей.
2. Каждый пользователь должен иметь уникальный идентификатор и пароль.
3. Пароли должны быть сложными и меняться периодически.
4. Предусмотрена блокировка учетной записи после нескольких неудачных попыток входа.
5. Должна быть возможность ограничения доступа к определенным функциям и данным в зависимости от роли пользователя.
6. Должны быть установлены правила для создания паролей и хранения их в зашифрованном виде.
7. Должны быть меры безопасности для защиты от несанкционированного доступа, такие как защита от взлома паролей и защита от вредоносных программ.
8. Должны быть установлены сроки действия учетных записей и паролей, а также правила для их обновления.

5.3 Требования к функциональной безопасности

1. Система должна обеспечивать контроль доступа к функциям и данным в зависимости от роли пользователя.
2. Система должна предусматривать автоматическое выход из системы после определенного периода неактивности.
3. Должен быть контроль доступа к системным ресурсам и функциям.
4. При возникновении сбоев в работе системы необходимо обеспечить сохранность данных.
5. При нескольких неудачных попытках входа учетная запись должна быть автоматически заблокирована.
6. Данные, передаваемые по сети, должны быть зашифрованы.
7. Система должна обеспечивать сохранность данных при сбоях в работе системы.

5.4 Требования к информационной безопасности

1. Аутентификация пользователей: система должна проверять подлинность пользователей перед предоставлением им доступа к защищенным ресурсам. Должна осуществлять с помощью протокола OAuth 2.
2. Система должна определять, какие действия могут выполнять пользователи.
3. Система должна гарантировать конфиденциальность информации, хранящейся в системе авторизации.
4. Система должна обеспечивать целостность данных, хранящихся в системе авторизации.
5. Система должна вести журнал событий и аудита для отслеживания действий пользователей и обнаружения возможных нарушений информационной безопасности.
6. Система должна иметь инструкцию работы в ней для пользователей.

5.5 Требования к патентной чистоте

1. Система автоматизации должна быть патентно чистой, то есть не нарушать права интеллектуальной собственности других лиц или организаций.
2. Все компоненты системы, включая программное обеспечение, аппаратное обеспечение и документацию, должны быть лицензированы и иметь соответствующие разрешения на использование.
3. При разработке системы должны соблюдаться стандарты и требования к защите интеллектуальной собственности.
4. Необходимо проводить регулярные проверки на наличие нарушений патентных прав и быстро реагировать на обнаруженные нарушения.
5. Регулярно проводите проверки на нарушения патентных прав и быстро реагируйте на обнаруженные нарушения.
6. Все сотрудники, участвующие в разработке и эксплуатации системы, должны быть обучены правилам защиты интеллектуальной собственности и осведомлены о возможных последствиях нарушения патентных прав.

6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

6.1 Требования к информационному обеспечению

1. Система должна быть легко настраиваемой, чтобы управляющий ее пользователь мог без труда изменять параметры системы.
2. Система авторизации должна быть масштабируемой, чтобы ее можно было легко расширять для работы с большим количеством пользователей.
3. Система должна предоставлять инструменты для мониторинга доступа и использования пользователей.
4. Система должна иметь права доступа в зависимости от роли, которой является пользователь.

6.2 Требования к математическому обеспечению

Требование не требуются.

6.3 Требования к программному обеспечению

1. Безопасность.
2. Простота использования.
3. Должно обеспечивать надежную работу системы.
4. Должно предоставлять возможность настройки различных методов аутентификации в соответствии с требованиями компании.
5. Должно быть совместимо с другими приложениями и системами.

6.9 Требования к техническому обеспечению

1. Система должна быть быстрой и отзывчивой для удобства пользователей.

2. Поддержка множества языков.

3. Защита от уязвимостей.

4. Устроения перечня возможных ошибок.

6.5 Требования к организационному обеспечению

1. Система авторизации должна иметь возможность управлять доступом пользователей к конкретным приложениям и ресурсам в зависимости от их роли и полномочий в организации.
2. Система авторизации должна соответствовать современным стандартам безопасности, таким как OAuth, OpenID Connect и SAML, чтобы обеспечить совместимость с другими системами и приложениями.
3. Система авторизации должна быть доступна для использования в любое время суток, чтобы пользователи могли получить доступ к необходимым ресурсам и приложениям без задержек.
4. Организация обучения пользователей.

7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ

8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ

1. Проведение тестовых мероприятий.
2. Разработка инструкции по работе системы.
3. Обучение сотрудников.

9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

1. Документация по установке, настройке и использованию системы авторизации
2. Описание функционала и особенностей работы системы
3. Инструкции по обновлению и расширению функционала системы.