МИНИСТЕРСТВО ТРАНСПОРТА И КОММУНИКАЦИЙ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования

«Белорусский государственный университет транспорта»

Кафедра «Управление эксплуатационной работой и охрана труда»

Отчет  
по лабораторной работе №6

по дисциплине «Средства и технологии анализа и разработки информационных систем»

Выполнил Проверил

студент группы ГИ-31 зав. каф. УЭРиОТ

Сидорова А. А. Козлов В. Г.

Гомель, 2025

# Лабораторная работа №6

# РАЗРАБОТКА ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ НА СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ

**Цель работы:** ознакомление с процессом разработки технического задания на создание автоматизированной системы (программного продукта).

**Задание:** разработка технический требований на создание автоматизированной системы аутентификации и авторизации в соответствии с СТП 09150.11.118-2009.

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

2 ОБЩИЕ СВЕДЕНИЯ

3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ

3.1 Назначение

3.2 Цели создания

4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ

5 ТРЕБОВАНИЯ К СИСТЕМЕ

5.1 Требования к структуре

5.2 Требования к процедурам доступа к системе

5.3 Требования к функциональной безопасности

5.4 Требования к информационной безопасности

5.5 Требования к патентной чистоте

6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

6.1 Требования к информационному обеспечению

6.2 Требования к математическому обеспечению

6.3 Требования к программному обеспечению

6.9 Требования к техническому обеспечению

6.5 Требования к организационному обеспечению

7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ

8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ

9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

**1 ВВЕДЕНИЕ**

Настоящий документ устанавливает технические требования к разработке автоматизированной системы аутентификации и авторизации (АСАА), предназначенной для обеспечения надежного, защищенного и удобного механизма идентификации пользователей при доступе к информационным ресурсам. Документ разработан в соответствии с требованиями СТП 09150.11.118-2009 и других нормативных актов, регламентирующих безопасность и защиту информации.

Автоматизированная система аутентификации и авторизации предназначена для управления доступом пользователей к корпоративным и ведомственным информационным системам, гарантируя высокий уровень защиты учетных данных. Разработка системы направлена на минимизацию рисков несанкционированного доступа, повышение удобства использования аутентификационных механизмов и обеспечение соответствия современным стандартам безопасности.

Настоящий документ содержит описание требований к структуре системы, функциональным и техническим характеристикам, а также регламентирует порядок её разработки, тестирования и ввода в эксплуатацию. В документе определены ключевые аспекты безопасности, механизмы хранения и обработки данных, а также методы защиты от потенциальных угроз.

Документ предназначен для использования разработчиками программного обеспечения, специалистами по информационной безопасности, администраторами систем, а также всеми заинтересованными сторонами, участвующими в процессе проектирования, внедрения и эксплуатации автоматизированной системы аутентификации и авторизации.

**2 ОБЩИЕ СВЕДЕНИЯ**

Технические требования определяют цели создания системы, требования к ее разработке, исходные данные, необходимые для проектирования, а также порядок внедрения системы. В документе приведены основные характеристики системы, требования к ее компонентам, а также описаны этапы разработки и внедрения.

Автоматизированная система аутентификации и авторизации предназначена для работы в различных информационных средах, включая локальные корпоративные сети, облачные платформы и распределенные системы. Она должна обеспечивать высокий уровень защиты персональных данных, а также соответствовать современным требованиям к информационной безопасности.

Разработка системы осуществляется с учетом интеграции с существующими информационными системами и возможностью масштабирования в зависимости от потребностей организации. Также учитываются требования по обеспечению отказоустойчивости, производительности и удобства использования для конечных пользователей.

*Таблица 2.1 –* **Основные компоненты системы**

|  |  |
| --- | --- |
| **Основные компоненты системы** | **Описание** |
| Модуль аутентификации | Проверка учетных данных пользователей |
| Модуль авторизации | Контроль прав доступа к ресурсам |
| Модуль восстановления пароля | Восстановление учетных записей пользователей |
| Журналирование событий | Логирование всех попыток входа в систему |
| Интеграция с внешними сервисами | Поддержка LDAP, Active Directory и других методов |

**3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ**

**3.1 Назначение**

Система предназначена для управления процессами аутентификации и авторизации пользователей в информационных системах, обеспечивая контроль доступа и защиту персональных данных. Реализация системы позволит снизить риски утечки учетных данных и повысить защищенность цифровых ресурсов.

* 1. **Цели создания**

Целями создания АСАА являются:

- Обеспечение безопасного входа пользователей в систему;

- Контроль прав доступа к ресурсам системы;

- Поддержка восстановления учетных данных;

- Обеспечение устойчивости системы к атакам на учетные записи пользователей;

- Обеспечение удобства использования при высоком уровне безопасности.

**4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ**

Объектами системы являются учетные записи пользователей и их данные, которые подлежат защите при входе в систему. К ним относятся:

* Идентификационные данные (логин, email);
* Аутентификационные данные (пароль, одноразовые коды);
* Логирование активности пользователей;
* Информация о правах доступа и ролях пользователей.

Система должна обеспечивать защиту всех объектов с использованием современных алгоритмов шифрования и механизмов управления доступом. В рамках разработки предусмотрено использование централизованного хранилища учетных данных с возможностью интеграции с внешними сервисами аутентификации.

**5 ТРЕБОВАНИЯ К СИСТЕМЕ**

**5.1 Требования к структуре**

Система должна включать:

* Модуль аутентификации (проверка учетных данных);
* Модуль авторизации (назначение прав доступа);
* Модуль восстановления пароля;
* Журналирование всех попыток входа в систему;
* Поддержку работы с различными уровнями доступа.

*Таблица 5.1 –* **Структура системы**

|  |  |
| --- | --- |
| **Компонент системы** | **Функция** |
| База данных пользователей | Хранение учетных записей пользователей в зашифрованном виде |
| Система логирования | Отслеживание и запись всех входов в систему |
| Модуль проверки паролей | Анализ соответствия пароля требованиям |

**5.2 Требования к процедурам доступа к системе**

- Вход в систему осуществляется с использованием логина и пароля;

- Пароль должен содержать не менее 8 символов, включая цифры и символы разного регистра;

- Проверка пароля на соответствие требованиям осуществляется на стороне клиента;

- После 10 минут бездействия сессия пользователя должна завершаться автоматически;

- Возможность многофакторной аутентификации (по SMS, email, аутентификатору).

**5.3 Требования к функциональной безопасности**

- Реализация механизма сброса и восстановления пароля;

- Контроль и учет попыток входа;

- Ограничение количества неудачных попыток входа;

- Поддержка механизма CAPTCHA при множественных неудачных попытках входа.

**5.4 Требования к информационной безопасности**

- Хранение паролей пользователей в зашифрованном виде (использование алгоритмов хеширования, например, bcrypt, Argon2);

- Использование защищенных каналов связи при передаче учетных данных (TLS, HTTPS);

- Регистрация и аудит всех входов в систему;

- Защита от атак типа «brute-force», SQL-инъекций и XSS.

*Таблица 5.2 –* **Методы защиты паролей**

|  |  |
| --- | --- |
| **Метод защиты** | **Описание** |
| Хеширование паролей | Использование bcrypt, Agron2 для безопасного хранения паролей |
| Защищенные соединения | Применение TLS/HTTPS для передачи данных |
| Ограничение попыток входа | Блокировка учетной записи при множественных неудачных попытках |

**5.5 Требования к патентной чистоте**

Отсутствуют.

**6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ**

**6.1 Требования к информационному обеспечению**

- База данных пользователей с зашифрованными учетными записями;

- Логирование всех операций аутентификации и авторизации;

- Поддержка интеграции с внешними источниками данных (LDAP, Active Directory).

**6.2 Требования к математическому обеспечению**

Отсутствуют.

**6.3 Требования к программному обеспечению**

- Поддержка работы в современных и устаревших версиях Windows/Linux;

- Использование стандартов безопасности OWASP;

- Совместимость с устаревшими версиями API;

- Совместимость с современными веб-браузерами и мобильными устройствами.

**6.9 Требования к техническому обеспечению**

Отсутствуют.

**6.5 Требования к организационному обеспечению**

Отсутствуют.

**7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ**

* Разработка программных компонентов системы;
* Проведение тестирования на безопасность;
* Разработка пользовательской документации;
* Внедрение системы в эксплуатацию;
* Обучение пользователей и администраторов.

**8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ**

Система считается принятой в эксплуатацию после успешного прохождения тестирования, устранения выявленных ошибок и подтверждения соответствия техническим требованиям. Тестирование включает:

* Проверку работоспособности основных функций системы;
* Оценку производительности и устойчивости к нагрузкам;
* Аудит безопасности и защиту данных.

**9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ**

В комплект документации должны входить:

* Руководство пользователя с инструкциями по использованию системы;
* Описание архитектуры системы и её компонентов;
* UML-диаграмма процессов аутентификации и авторизации;
* Отчет по результатам тестирования системы.