**ЛАБОРАТОРНАЯ РАБОТА №4**

РАЗРАБОТКА ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ НА СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ

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

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

В настоящем документе описываются требования к созданию автоматизированной системы аутентификации и авторизации в соответствии с требованиями СТП 09150.11.118-2009. Данная система разрабатывается с целью обеспечения безопасного доступа к информационным ресурсам и контроля прав доступа пользователей.

2 ОБЩИЕ СВЕДЕНИЯ

1. Наименование работы: разработка технических требований на автоматизированную систему аутентификации и авторизации в соответствие с СТП 09150.11.118-2009 (АС АиА).
2. Заказчик АС и Ответственный по проекту: заказчик АС – Государственное объединение «Белорусская железная дорога»; Ответственный по проекту – Служба информационных технологий Государственного объединения «Белорусская железная дорога».
3. Наименование Организации-пользователя АС: Государственное объединение «Белорусская железная дорога».
4. Наименование объекта внедрения: службы и подразделения Белорусской железной дороги, ИС Белорусской железной дороги.

3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ

3.1 Назначение: Назначение разработки АС аутентификации и авторизации для сотрудников и пользователей информационной системы состоит в обеспечении безопасного доступа к информационным ресурсам компании.

Разработка такой системы поможет повысить уровень безопасности информационных ресурсов и защитить конфиденциальные данные компании от несанкционированного доступа, обеспечивая эффективное функционирование информационной.

3.2 Цели создания: Разработка преследует следующие цели и задачи:

* Обеспечение безопасности. Система должна гарантировать, что только авторизованные пользователи могут получить доступ к конфиденциальным данным и ресурсам компании, предотвращая несанкционированный доступ и потенциальные угрозы безопасности.
* Управление доступом. Автоматизированная система позволяет управлять правами доступа сотрудников и пользователей, определяя, к каким данным и функциям каждый из них имеет доступ в соответствии с их ролью и обязанностями.
* Удобство использования. Создание простого и удобного интерфейса для аутентификации и авторизации упрощает процесс работы с информационными системами, повышая эффективность и производительность сотрудников.
* Мониторинг и аудит. Система должна предоставлять возможность отслеживать действия пользователей, регистрировать входы и выходы, а также анализировать активность для выявления аномалий и возможных угроз безопасности.
* Соблюдение нормативов. Разработка системы аутентификации и авторизации должна учитывать соблюдение соответствующих нормативов и стандартов в области безопасности информации и защиты персональных данных.

4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ

Автоматизация процессов авторизации и аутентификации представляет собой внедрение специализированных программных средств для упрощения и обеспечения безопасности доступа к информационным ресурсам.

Объекты автоматизации – процессы аутентификации и авторизации пользователей в ИС Белорусской железной дороги.

Участники данных процессов – это: ­

* пользователи информационно-телекоммуникационной сети «Интернет», незарегистрированные в ЕСИА; ­
* работники структурных подразделений Белорусской железной дороги; ­

Автоматизированные системы аутентификации, такие как одноразовые пароли, биометрическая идентификация или многофакторная аутентификация, повышают уровень безопасности за счет точности и сложности проверки подлинности.

Автоматизация процесса авторизации позволяет быстро и точно определить права доступа пользователя к различным ресурсам, что снижает вероятность ошибок и угроз безопасности.

ИС подразумевает доступ пользователей к системе в режиме «клиент-сервер», с использованием Web технологий.

5 ТРЕБОВАНИЯ К СИСТЕМЕ

5.1 Требования к структуре: В качестве платформы для построения АС должно использоваться программное обеспечение с открытым исходным кодом. Проектирование АС должно базироваться на сервисно-ориентированной архитектуре:

* уровень представления информации;
* уровень прикладной бизнес логики;
* уровень транспортировки сервисов;
* уровень хранения и обработки данных (сервер базы данных).

Система должна быть построена с использованием модульной архитектуры, позволяющей легко добавлять новые методы аутентификации и авторизации, а также интегрировать её с другими информационными системами и сервисами.

5.2 Требования к процедурам доступа к системе: Пользователи должны проходить процедуру регистрации, включающую проверку личности и установку уникального идентификатора (логина) и пароля. Пароль пользователя должен быть не менее 8 символов и обязательно содержать цифры и символы разного регистра. Такие же требования используются при аутентификации.

Проверка пароля на соответствие требованиям должна осуществляться на стороне клиента.

Система должна поддерживать различные методы аутентификации, включая парольные, биометрические, одноразовые пароли и многофакторную аутентификацию.

Администраторы должны иметь возможность управлять правами доступа пользователей в соответствии с их ролями и обязанностями в организации.

Процедуры управления доступом должны быть прозрачными и гибкими, позволяя быстро реагировать на изменения в структуре организации и потребности пользователей.

Пользователи, обладающие доступом к конфиденциальным данным или критическим ресурсам, должны проходить многофакторную аутентификацию для повышения уровня безопасности.

Пользователи должны быть ознакомлены с политиками безопасности, регламентирующими правила использования системы и обязанности пользователей по обеспечению безопасности информации.

Максимальный период неактивности пользователя – 10 минут. После этого сессия уничтожается, пользователь должен вновь вводить логин и пароль.

5.3 Требования к функциональной безопасности: Система должна обеспечивать защиту от несанкционированного доступа путем эффективного управления аутентификацией и авторизацией пользователей.

Должны быть реализованы меры по предотвращению атак перебора паролей, подбора идентификаторов и других типов атак на аутентификацию.

Система должна обеспечивать гранулярный контроль доступа к ресурсам на основе ролей, прав и политик безопасности.

Должны быть предусмотрены механизмы аудита и мониторинга, позволяющие отслеживать действия пользователей и выявлять подозрительную активность.

Система должна обеспечивать шифрование паролей, чтобы защитить пользователей от несанкционированного доступа.

Должны использоваться современные алгоритмы шифрования и протоколы безопасности для обеспечения надежной защиты паролей.

Процедура многофакторной аутентификации может включать использование пароля в сочетании с SMS-кодом, аутентификационным приложением или биометрическим сканером.

Система должна обрабатывать ошибки и исключения безопасным образом, чтобы предотвращать утечку чувствительной информации и иные нарушения безопасности.

Должны быть предусмотрены механизмы резервного копирования и восстановления данных для обеспечения доступности информации в случае аварийных ситуаций или сбоев.

Должны быть предусмотрены варианты сброса пароля, либо же восстановления данных по заранее введенной информации. Должны использоваться логин, адрес электронной почты или номер телефона.

5.4 Требования к информационной безопасности: Данные пользователей, включая учетные записи и пароли, должны храниться и передаваться в зашифрованном виде.

Должны быть приняты меры для защиты информации от несанкционированных изменений или повреждений.

Должны использоваться методы хэширования для обеспечения целостности хранимых данных и их защиты от подмены или искажения.

Система должна обеспечивать доступность информации для авторизованных пользователей в том случае, если это необходимо для нормального функционирования бизнес-процессов.

Должны быть предусмотрены меры по обеспечению доступности системы в случае возникновения аварийных ситуаций или атак на доступность.

Система должна защищаться от различных угроз, включая внешние атаки (например, DDoS-атаки), внутренние угрозы (например, утечки данных) и другие типы атак.

Должны быть приняты меры по обнаружению и предотвращению угроз, а также механизмы реагирования на инциденты безопасности.

Система должна регулярно обновляться и мониториться на наличие уязвимостей и потенциальных угроз безопасности.

Должны быть приняты меры по оперативному реагированию на обнаруженные уязвимости и обновлению системы для их исправления.

5.5 Требования к патентной чистоте: При проектировании системы следует предпочтительно использовать открытые стандарты и протоколы, которые не защищены патентами и свободно доступны для использования.

Если необходимо использовать патентно-защищенные методы или технологии, следует убедиться в наличии соответствующих лицензий или разрешений на их использование.

Если в ходе разработки системы ведется сотрудничество с третьими сторонами или исполнителями, необходимо заключить с ними соглашения о неразглашении, чтобы предотвратить возможные споры относительно интеллектуальной собственности.

Все этапы проверки патентной чистоты и принятые меры по обеспечению соблюдения патентного законодательства должны быть документированы для последующего аудита и подтверждения соответствия.

6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

6.1 Требования к информационному обеспечению:

* Хранение пользовательских данных. Система должна обеспечивать безопасное и надежное хранение пользовательских данных, таких как идентификационная информация, учетные записи и пароли. Для этого необходимо использовать современные методы шифрования.
* Методы аутентификации. Система должна поддерживать различные методы аутентификации, такие как парольная аутентификация, с использованием одноразовых паролей(ОТР), биометрическая аутентификация.
* Управление сессиями. Система должна обеспечивать безопасное управление сеансами пользователей, включая контроль времени сеанса, защиту от атак перехвата сеансов и возможность завершения сеанса при выходе пользователя.
* Аудит и журналирование. Система должна вести аудит и журналирование всех действий пользователей, включая попытки входа, изменения прав доступа и другие события, с целью обеспечения контроля и обнаружения инцидентов безопасности.
* Защита от атак. Информационное обеспечение должно включать механизмы защиты от распространенных видов атак таких как SQL-инъекций, кросс-сайтовый скриптинг и межсайтовая подделка запросов, а также предоставлять защиту от DDoS-атак и других угроз.
* Обновление и обслуживание. Система должна иметь механизмы для регулярного обновления и обслуживания информационного обеспечения, включая патчи безопасности и обновления программного обеспечения.

6.2 Требования к программному обеспечению:

Надежность и стабильность. Программное обеспечение должно быть надежным и стабильным, обеспечивая бесперебойную работу системы. Это включает в себя обработку ошибок, предотвращение сбоев и восстановление после отказов.

Совместимость. Программное обеспечение должно быть совместимо с другими компонентами информационной инфраструктуры организации, а также с различными операционными системами, браузерами и устройствами.

Масштабируемость. Программное обеспечение должно обеспечивать возможность масштабирования системы в зависимости от изменяющихся потребностей организации, включая увеличение числа пользователей, объема данных и нагрузки на систему.

Безопасность. Программное обеспечение должно обеспечивать высокий уровень безопасности, включая защиту от атак, уязвимостей и утечек данных.

6.3 Требования к техническому обеспечению

Производительность. Система должна быть развернута на высокопроизводительном оборудовании, способном обрабатывать большие объемы запросов с минимальными задержками.

Отказоустойчивость. Техническое обеспечение должно быть отказоустойчивым, обеспечивая непрерывную работу системы даже в случае отказа отдельных компонентов или сетевых подключений

6.4 Требования к организационному обеспечению

Управление проектом. Должен быть определен ответственный руководитель проекта, который будет координировать все этапы разработки, внедрения и поддержки системы. Также необходимо иметь четкий план с определенными сроками и ресурсами.

Разделение обязанностей. Определение ролей и ответственностей различных участников проекта, включая разработчиков, тестировщиков, администраторов и конечных пользователей. Каждый должен понимать свои обязанности и выполнять их эффективно.

Обучение и поддержка персонала. Обеспечение обучения персонала по использованию и администрированию системы аутентификации и авторизации, а также предоставление технической поддержки при необходимости.

7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ

Подготовительный этап:

* Проверка наличия всех необходимых документов (техническое задание, руководства, планы тестирования).

Тестирование системы:

* Проведение функционального тестирования для проверки соответствия системы требованиям технического задания.
* Выполнение нагрузочного тестирования для оценки производительности системы при пиковых нагрузках.
* Проведение тестов безопасности для проверки устойчивости системы к внешним угрозам.

Исправление выявленных недостатков:

* Устранение обнаруженных в ходе тестирования ошибок и недочетов.
* Повторное тестирование для подтверждения исправления недостатков.

Проверка документации:

* Проверка полноты и актуальности технической и эксплуатационной документации.

Пилотная эксплуатация:

* Временное внедрение системы в ограниченном объеме для оценки ее работы в реальных условиях.
* Мониторинг работы системы и сбор обратной связи от пользователей.

Финальная приемка:

* Оценка результатов пилотной эксплуатации.
* Подписание актов о приемке системы заказчиком и исполнителем.
* Передача системы в постоянную эксплуатацию.

Постприемочное сопровождение:

* Организация технической поддержки и сервисного обслуживания системы.

Планирование дальнейших обновлений и модернизации системы.

8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ

* Стандартизация ‒ документация должна быть выполнена в соответствии с принятыми стандартами.
* Ясность и понятность ‒ информация должна быть изложена ясно и понятно для всех участников проекта.
* Полнота ‒ документация должна полностью отражать все аспекты системы, включая требования, архитектуру, код, тестовые процедуры и результаты.
* Доступность ‒ документы должны быть легкодоступны для всех членов команды и заинтересованных сторон.
* Актуальность ‒ документация должна регулярно обновляться для отражения текущего состояния проекта.
* Идентификация версий ‒ все изменения в документации должны сопровождаться обновлением версии документа.
* Безопасность ‒ документация должна храниться в безопасном месте с контролем доступа.

Утверждение ‒ все ключевые документы должны проходить процедуру утверждения ответственными лицами.

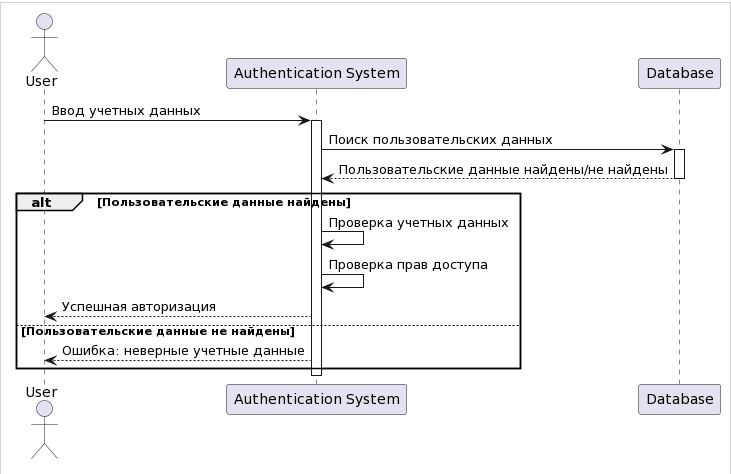


Рисунок 1 ‒ Диаграмма последовательности