**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).

**Тема проект:** разработка технический требований на создание

автоматизированной системы аутентификации и авторизации в соответствии с

СТП 09150.11.118-2009.

**Технические требования:**

- процесс аутентификации и авторизации должен осуществляться через

запрос данных учетной записи (логин и пароль) пользователя.

- пароль пользователя должен быть не менее 8 символов и обязательно

содержать цифры и символы разного регистра. Проверка пароля на соответствие

требованиям должно осуществляться на стороне клиента;

- хранение пароля пользователя в системе должно осуществляться в

зашифрованном виде;

- при отсутствии активности пользователя в системе более 10 минут

уничтожается сессия;

- предусмотреть подсистему сброса и восстановления данных учетной записи

пользователя;

- предусмотреть UML-диаграмму процесса аутентификации и авторизации

пользователя в системе.

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

6.4 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**

Целью данного документа является определение технических требований к разработке автоматизированной системы аутентификации и авторизации для предприятия Гомельэнерго. Эта система необходима для обеспечения безопасного доступа пользователей к информационным ресурсам предприятия.

Автоматизированная система аутентификации и авторизации предполагает создание механизма, который позволит пользователям предприятия Гомельэнерго идентифицировать себя перед доступом к информационным системам и ресурсам, а также управлять своими правами доступа.

Предприятие Гомельэнерго является одним из крупнейших энергетических предприятий, включающим в себя различные информационные системы, базы данных и важные цифровые ресурсы. Безопасность доступа к этим ресурсам критически важна для защиты конфиденциальности и целостности информации, а также для обеспечения бесперебойной работы предприятия.

**2.ОБЩИЕ СВЕДЕНИЯ**

Проект разработки автоматизированной системы аутентификации и авторизации для предприятия Гомельэнерго взаимодействует с существующими информационными системами предприятия, такими как электронная почта, корпоративные порталы и базы данных сотрудников. Система будет функционировать как ключевой элемент для обеспечения безопасного доступа сотрудников к цифровым ресурсам и приложениям предприятия.

Функции продукта включают:

* Аутентификацию пользователей посредством запроса данных учетной записи (логин и пароль) из корпоративной базы данных сотрудников.
* Хранение и обработку учетных данных сотрудников в зашифрованном виде на серверах предприятия.
* Управление активными сессиями пользователей и автоматическое завершение неактивных сеансов после 10 минут бездействия.
* Механизм сброса и восстановления данных учетной записи, доступный через корпоративный портал для сотрудников.

Характеристики пользователей системы включают сотрудников предприятия Гомельэнерго с различными уровнями доступа к информационным ресурсам и приложениям. Пользователи обязаны соблюдать политику безопасности предприятия и использовать сложные пароли для доступа к системе.

Ограничения, допущения и зависимости:

* Система зависит от доступа к внутренней сети предприятия для обмена данными с серверами и другими компонентами информационной инфраструктуры.
* Ограничения могут быть связаны с соблюдением политики безопасности предприятия и требованиями к защите конфиденциальной информации.
* Допущения включают предположение о том, что сотрудники будут активно использовать систему для доступа к информационным ресурсам предприятия и соблюдать правила безопасности при работе с учетными данными.

**3.НАЗНАЧЕНИЕ**

**3.1 Назначение**

Назначением создания автоматизированной системы аутентификации и авторизации для предприятия Гомельэнерго является обеспечение безопасного и эффективного доступа пользователей к информационным ресурсам предприятия. Система предназначена для усиления контроля доступа к цифровым данным и ресурсам, а также для предотвращения несанкционированного доступа и утечек конфиденциальной информации.  
**3.2 Цели создания**

Основными целями создания системы являются:

* Повышение безопасности: Реализация механизмов аутентификации и авторизации с использованием современных методов шифрования и проверки подлинности поможет защитить информацию от несанкционированного доступа и утечек.
* Улучшение управления доступом: Предоставление сотрудникам удобного и безопасного способа доступа к информационным ресурсам предприятия, управление правами доступа и сессиями пользователей.
* Соблюдение законодательных требований и стандартов безопасности: Гарантирование соответствия системы авторизации и аутентификации требованиям законодательства и стандартам безопасности, в том числе в области защиты персональных данных и конфиденциальной информации.

**3.3 Характеристика объекта автоматизации**

Объектом автоматизации являются процессы аутентификации и авторизации пользователей предприятия Гомельэнерго при доступе к информационным системам, базам данных и цифровым ресурсам предприятия. Система должна обеспечивать безопасный, удобный и эффективный доступ сотрудников к необходимой информации, учитывая различные уровни доступа и права пользователей.

**4. ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ**

**4.1 Общие сведения**

В данном разделе приведена общая информация о пункте, информация о перечнях и краткие характеристики бизнес-процессов в системе, требования к входным и выходным данным, формам их представления, а также выполняемым технологическим операциям.

**4.2 Перечень и краткая информация бизнес-процессов**

1. Процесс аутентификации и авторизации:

Включает запрос данных учетной записи пользователя, проверку пароля, управление сессиями и механизм сброса данных учетной записи.

2. Управление учетными записями пользователей:

Включает создание, изменение, блокировку и удаление учетных данных пользователей, а также управление их правами доступа.

**4.3 Требования к входным и выходным данным, формам их представления**

В данном пункте уточняются ожидаемые форматы и структуры входных и выходных данных для каждого бизнес-процесса. Входные данные должны быть представлены в соответствии с определенными форматами, а выходные данные должны быть информативными и удобными для дальнейшей обработки.

Входные данные:

* Логин и пароль пользователя для процесса аутентификации.
* Данные учетной записи для управления учетными данными пользователей.

Выходные данные:

* Результаты аутентификации и авторизации.
* Информация о состоянии и изменениях учетных записей пользователей.

Данные представляются в текстовом и графическом форматах через веб-интерфейс системы для аутентификации и авторизации, а также через административный интерфейс для управления учетными записями.

**4.4 Выполняемые технологические операции**

Технологические операции описывают основные действия, выполняемые системой для обработки данных и управления процессами. Каждая операция выполняется в соответствии с определенными алгоритмами и процедурами, обеспечивающими корректное функционирование системы.

Выполняемые технологические операции:

* Запрос данных учетной записи пользователя.
* Проверка пароля на соответствие требованиям.
* Шифрование и хранение учетных данных в защищенном формате.
* Управление сессиями пользователей.
* Создание, изменение, блокировка и удаление учетных записей.

**5. ТРЕБОВАНИЯ К СИСТЕМЕ**

**5.1 Требования к структуре**

Система должна быть построена на модульной структуре, обеспечивающей гибкость и масштабируемость. Каждый модуль должен иметь четко определенные функции и интерфейсы для взаимодействия с другими модулями.

**5.2 Требования к процедурам доступа к системе**

Система должна обеспечивать процесс аутентификации и авторизации через запрос данных учетной записи (логин и пароль) пользователя, используя криптографические методы для защиты передаваемых данных.

При отсутствии активности пользователя в системе более 10 минут, система должна автоматически завершать сессию пользователя и требовать повторной аутентификации для возобновления работы.

Предусмотрена подсистема сброса и восстановления данных учетной записи пользователя, предоставляющая безопасный и авторизованный доступ к этим процессам.

**5.3 Требования к функциональной безопасности**

Система должна проводить проверку на безопасность всех входящих данных, включая вводимые пользователем данные, и предотвращать возможность атак на аутентификационные механизмы.

Обеспечить механизм для обнаружения и автоматического блокирования подозрительной активности пользователей, включая анализ необычных попыток входа или доступа к ресурсам, основанный на поведенческих и аналитических данных.

Пароль пользователя должен соответствовать следующим критериям:

* Быть не менее 8 символов в длину.
* Содержать как минимум одну цифру.
* Содержать символы разного регистра.

Проверка пароля на соответствие данным требованиям должна осуществляться на стороне клиента перед передачей на сервер.

Хранение пароля пользователя в системе должно осуществляться в зашифрованном виде с использованием надежных алгоритмов шифрования.

Регулярное выражение для проверки формата ввода пароля может быть следующим:

^(?=.\*\d)(?=.\*[a-z])(?=.\*[A-Z]).{8,}$

Оно необходимо для обеспечения безопасности пароля путем применения определенных правил, таких как минимальная длина, наличие цифр и символов верхнего и нижнего регистра. Пароль, соответствующий этому регулярному выражению, будет обладать высокой степенью сложности и труднодоступности для злоумышленников.

Данное регулярное выражение состоит из:

* ^: Символ начала строки.
* (?=.\*\d): Положительное предварительное условие (positive lookahead), гарантирующее наличие хотя бы одной цифры.
* (?=.\*[a-z]): Еще одно положительное предварительное условие, гарантирующее наличие хотя бы одной буквы в нижнем регистре.
* (?=.\*[A-Z]): Положительное предварительное условие, гарантирующее наличие хотя бы одной буквы в верхнем регистре.
* .{8,}: Любые символы (кроме символа новой строки) длиной не менее 8.
* $: Символ конца строки.

Это регулярное выражение гарантирует, что пароль будет состоять из минимум восьми символов, содержать как минимум одну цифру, одну букву в нижнем регистре и одну букву в верхнем регистре.

**5.4 Требования к информационной безопасности**

Система должна обеспечивать защиту конфиденциальности данных пользователей путем использования механизмов шифрования и управления доступом.

Реализовать механизмы резервного копирования и восстановления данных для обеспечения их целостности и доступности в случае сбоев или атак.

**5.5 Требования к патентной чистоте**

При разработке системы необходимо соблюдать авторские права и патентные законы, исключая использование патентно защищенных методов или алгоритмов без соответствующих лицензий.

**6. ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ**

**6.1 Требования к информационному обеспечению**

К информационному обеспечению предъявляются следующие общие требования:

* информационное обеспечение должно быть достаточным для поддержания всех автоматизируемых функций объекта;
* для кодирования информации должны использоваться принятые у заказчика классификаторы;
* для кодирования входной и выходной информации, которая используется на высшем уровне управления, должны быть использованы классификаторы этого уровня;
* должна быть обеспечена совместимость с информационным обеспечением систем, взаимодействующих с разрабатываемой системой;
* структура экранных форм должна соответствовать характеристикам терминалов на рабочих местах конечных пользователей;
* графики формирования и содержание информационных сообщений, а также используемые аббревиатуры должны быть общеприняты в этой предметной области и согласованы с заказчиком;
* в ИС должны быть предусмотрены средства контроля входной и результатной информации, обновления данных в информационных массивах, контроля целостности информационной базы, защиты от несанкционированного доступа.

**6.2 Требования к математическому обеспечению**

Система должна использовать надежные математические алгоритмы шифрования для защиты паролей пользователей и других конфиденциальных данных.

Выбранные алгоритмы должны быть хорошо исследованы и признаны стойкими к различным атакам.

Для хранения паролей в зашифрованном виде система должна применять криптографические хэш-функции.

Эти функции должны обеспечивать невозможность восстановления исходного пароля из его хэша, а также быть устойчивыми к коллизиям.

**6.3 Требования к программному обеспечению**

Разработать программное обеспечение для реализации аутентификационных и авторизационных механизмов.

Обеспечить поддержку современных стандартов криптографии для защиты данных пользователей.

**6.4 Требования к техническому обеспечению**

Техническое обеспечение системы должно максимально и наиболее эффективным образом использовать существующие технические средства.

В состав комплекса должны входить следующие технические средства:

1) сервер БД;

2) персональные компьютеры (ПК) пользователей.

Минимальные требования к характеристикам компонентов технического обеспечения, при которых значения временных параметров Системы должны соответствовать предъявленным в ТЗ требованиям:

Для сервера БД:

* процессор – 2 х IntelXeon3 ГГц;
* объем оперативной памяти – 16 Гб;
* дисковая подсистема – 4 х 146 Гб;
* устройство чтения компакт-дисков (DVD-ROM);
* сетевой адаптер – 100 Мбит/с.

Для ПК пользователя:

* процессор – IntelPentium1.5 ГГц;
* объем оперативной памяти – 256 Мб;
* дисковая память – 40 Гб;
* сетевой адаптер – 100 Мбит/с.

**6.5 Требования к организационному обеспечению**

Обеспечить поддержку и обновление системы аутентификации и авторизации со стороны IT-отдела предприятия.

Организовать процессы мониторинга и анализа безопасности системы с участием специалистов по информационной безопасности.

**7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ**

**7.1 Проведение анализа и сбор информации**

Исследование требований и потребностей предприятия к системе аутентификации и авторизации.

Сбор и анализ данных о текущих процессах аутентификации и авторизации.

Определение функциональных и нефункциональных требований к системе.

**7.2 Разработка проекта системы**

Разработка архитектуры системы аутентификации и авторизации, включая выбор технологий и инструментов.

Создание диаграмм для описания работы системы.

Проектирование структуры базы данных для хранения пользовательских данных и прав доступа.

**7.3 Реализация и тестирование**

Написание программного кода для модулей аутентификации, авторизации и управления пользователями.

Разработка пользовательского интерфейса для взаимодействия с системой.

Тестирование разработанных модулей на соответствие требованиям и надежность работы.

**7.4 Интеграция и внедрение**

Интеграция разработанных модулей с существующей информационной инфраструктурой предприятия.

Проведение интеграционного тестирования для проверки работы системы в целом.

Внедрение системы на предприятии с обучением пользователей и администраторов.

**7.5 Поддержка и обслуживание**

Предоставление технической поддержки и сопровождения системы после внедрения.

Регулярное обновление и доработка системы в соответствии с потребностями предприятия.

Мониторинг работы системы и оперативное реагирование на возникающие проблемы и инциденты.

**7.6 Оценка эффективности**

Проведение оценки эффективности внедренной системы на основе достигнутых результатов и удовлетворения потребностей предприятия.

**8. ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ**

**8.1 Подготовка к приемке**

Сбор необходимой документации, включая акты внедрения системы и техническую документацию.

Проверка готовности всех компонентов системы к эксплуатации.

**8.2 Проведение приемочных испытаний**

Тестирование системы для проверки соответствия требованиям и качеству работы.

**8.3 Устранение замечаний и несоответствий**

Работа по устранению выявленных проблем и несоответствий.

**8.4 Передача системы в эксплуатацию**

Подготовка к эксплуатации системы, включая настройку и обучение пользователей.

Передача всех необходимых доступов и прав для работы с системой.

**8.5 Мониторинг и поддержка**

Организация регулярного мониторинга работы системы и предоставление технической поддержки пользователям.

**9. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ**

**9.1 Техническая документация**

Создание технической спецификации: Необходимо разработать подробную техническую спецификацию, которая содержит описание архитектуры системы, используемые технологии, алгоритмы аутентификации и авторизации, а также методы шифрования.

Формирование диаграмм: Для наглядного представления структуры и работы системы требуется создание диаграмм классов, взаимодействия и последовательности.

**9.2 Руководства пользователя**

Подготовка руководства пользователя: Разработка понятного и доступного руководства, которое содержит информацию о процедурах регистрации, входа в систему, восстановления пароля и управления учетной записью.

Формирование FAQ: Дополнительно к руководству рекомендуется создание FAQ с часто задаваемыми вопросами для быстрого решения типичных проблем и ситуаций.

**9.3 Руководства администратора**

Описание процедур управления системой: Подготовка документации, которая описывает процедуры управления системой со стороны администраторов. Это включает в себя установку прав доступа, мониторинг безопасности и реагирование на инциденты.

**9.4 Тестовая документация**

Подготовка плана тестирования: Разработка детального плана тестирования, который включает в себя описание тестовых сценариев, критериев приемки и ожидаемых результатов.

Формирование отчетов о тестировании: После проведения тестирования необходимо составить отчеты о его результатах, в которых описываются выявленные ошибки, аномалии и рекомендации по их исправлению.

**ПРИЛОЖЕНИЕ А**

Диаграмма последовательности в нотации UML для изображения аутентификации и авторизации в системе.

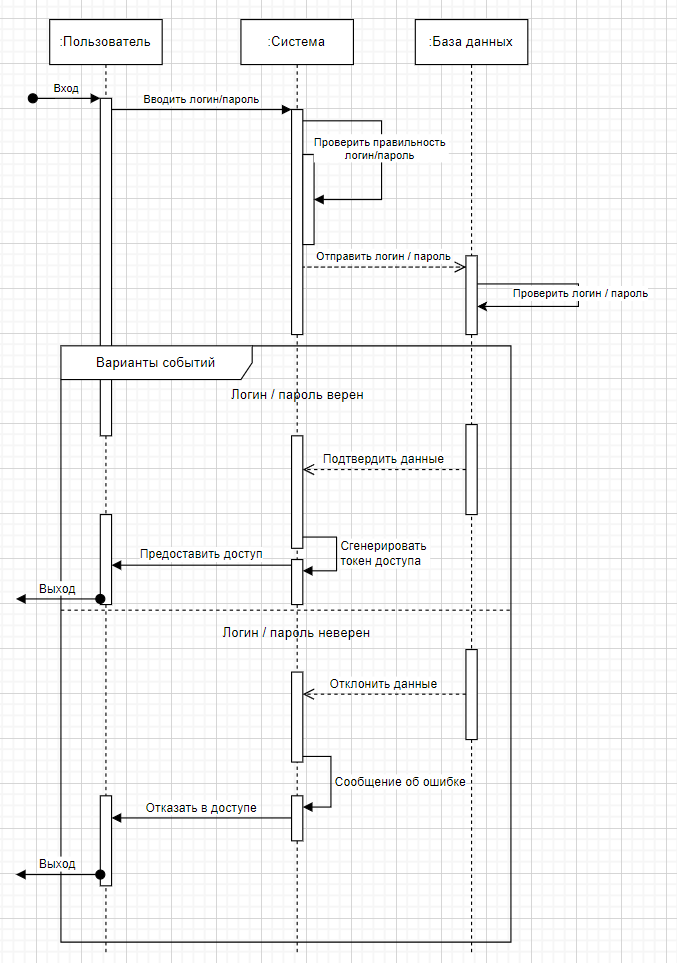


Рисунок 1 – Диаграмма последовательности