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 проекта**: 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

4.1 Перечень и краткая характеристика бизнес-процессов

4.2 Требования к входным и выходным данным, формам их представления

4.2.1 Требования к входным данным

4.2.2 Требования к выходным данным

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

6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

6.1 Требования к информационному обеспечению

6.2 Требования к программному обеспечению

6.3 Требования к техническому обеспечению

7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ

8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ

9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

1. ВВЕДЕНИЕ

С развитием информационных технологий и увеличением объемов цифровой информации, обеспечение безопасности корпоративных ресурсов и данных становится приоритетной задачей для современных предприятий. ОАО "Нафтан" не является исключением, поскольку сохранность конфиденциальной информации и предотвращение несанкционированного доступа имеют важное значение для успешной деятельности предприятия.

Цель данного проекта заключается в разработке и внедрении современной системы аутентификации и авторизации на предприятии ОАО "Нафтан", которая обеспечит надежную защиту информационных ресурсов, эффективный контроль доступа к данным и соблюдение стандартов информационной безопасности. Создание такой системы позволит минимизировать риски утечки конфиденциальной информации, обеспечить целостность и доступность данных, а также повысить общую производительность и эффективность работы предприятия.

Данное техническое задание определяет основные требования к созданию автоматизированной системы аутентификации и авторизации на основе передовых технологий информационной безопасности. В процессе реализации проекта будет уделено особое внимание выбору подходящих технологических решений, интеграции с существующей инфраструктурой предприятия и обеспечению максимального уровня безопасности и надежности системы.

Реализация данного проекта представляет собой важный шаг в повышении уровня информационной безопасности на предприятии ОАО "Нафтан" и будет способствовать достижению целей в области защиты данных и обеспечения безопасности информационных ресурсов в современных условиях деятельности организации.

1. ОБЩИЕ СВЕДЕНИЯ

Технические требования на разработку автоматизированной системы (ТТ) –

документ, оформленный в установленном порядке и определяющий цели

создания автоматизированной системы, детальные требования к разработке/модернизации автоматизированной системы, исходные данные,

необходимые для ее разработки, а также план-график создания автоматизированной системы.

1. **Автоматизированная система (АС):** Совокупность взаимосвязанных компонентов, включающая программное обеспечение, аппаратное обеспечение, базы данных, средства связи и пользовательские интерфейсы, предназначенная для автоматизации определенных бизнес-процессов или задач с целью повышения эффективности работы и улучшения качества предоставляемых услуг.

2. **Технические требования (ТТ):** Документ, формализующий необходимые характеристики, функциональные и нефункциональные особенности, а также критерии качества и производительности, которым должна соответствовать разрабатываемая или модернизируемая система, чтобы удовлетворить потребности заказчика и обеспечить эффективное функционирование системы.

1. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ

**3.1 Назначение**

Целью внедрения автоматизированной системы на предприятии ОАО "Нафтан" является повышение уровня безопасности информационных ресурсов, эффективное управление доступом к конфиденциальным данным и оптимизация бизнес-процессов в соответствии с современными стандартами информационной безопасности и требованиями предприятия.

Ключевые назначения автоматизированной системы включают в себя:

1. **Обеспечение безопасности данных:** Система будет обеспечивать защиту конфиденциальной информации, предотвращая несанкционированный доступ и минимизируя риски утечки данных.

2. **Управление доступом:** Автоматизированная система позволит централизованно управлять пользователями, их ролями и правами доступа к информационным ресурсам предприятия, обеспечивая необходимый уровень привилегий в соответствии с должностными обязанностями.

3. **Повышение оперативности:** Система позволит быстро и эффективно реагировать на изменения в требованиях безопасности, а также обеспечит оперативный мониторинг и контроль за доступом к информационным ресурсам предприятия.

В целом, внедрение автоматизированной системы на предприятии ОАО "Нафтан" направлено на повышение безопасности и эффективности работы, сокращение рисков и обеспечение надежной защиты цифровых активов предприятия.

**3.2 Цели создания**

Цели создания автоматизированной системы на предприятии ОАО "Нафтан" включают в себя:

* Обеспечение высокого уровня безопасности и защиты конфиденциальной информации предприятия.
* Реализация эффективного управления доступом к информационным ресурсам с учетом должностных обязанностей сотрудников.
* Оптимизация бизнес-процессов путем сокращения времени на аутентификацию и авторизацию.
* Соответствие системы требованиям законодательства и стандартам безопасности.
* Повышение ответственности и прозрачности в управлении доступом к информации.

1. ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ

**4.1 Перечень и краткая характеристика бизнес-процессов**

1. **Процесс аутентификации и авторизации пользователей:** обеспечивает идентификацию пользователей и предоставление им доступа к информационным ресурсам в соответствии с их ролями и правами.

2. **Процесс управления доступом к данным:** позволяет определить права доступа к различным видам информации в зависимости от роли и полномочий пользователя.

3. **Процесс резервного копирования и восстановления данных:** осуществляет регулярное создание резервных копий информационных ресурсов и обеспечивает их восстановление в случае необходимости.

4. **Процесс управления конфигурацией и обновлений:** обеспечивает контроль и управление изменениями в конфигурации системы, а также регулярное внедрение обновлений и исправлений безопасности.

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

**4.2.1 Требования к входным данным**

**Идентификационные данные пользователя**:

Система должна принимать идентификационные данные пользователей, такие как логин, электронная почта, номер телефона или другие атрибуты, необходимые для процесса аутентификации. Данные должны быть введены пользователем через специальные формы на веб-странице, мобильном приложении или другом интерфейсе.

**Пароль или другие учетные данные**

Система должна получать пароль или другие учетные данные, которые будут использоваться для проверки подлинности пользователя во время процесса аутентификации. Пароль должен быть введен пользователем в защищенной форме, например, через поле ввода пароля на веб-странице или в мобильном приложении.

**4.2.2 Требования к выходным данным**:

**Статус аутентификации пользователя**

Система должна предоставлять информацию о результате процесса аутентификации пользователя, указывая успешность или неуспешность проверки подлинности. Выходные данные могут содержать текстовые сообщения или коды состояния, указывающие на результат процесса аутентификации.

**Права доступа пользователя**

Система должна возвращать информацию о правах доступа пользователя к ресурсам системы после успешной аутентификации и авторизации. Права доступа могут быть представлены в виде списка ролей, групп или разрешений, соответствующих конкретным функциональным возможностям системы.

1. ТРЕБОВАНИЯ К СИСТЕМЕ
   1. **Требования к структуре**
2. **“Клиент-сервер”**

Система должна быть вида “клиент-сервер”, где клиент посылает запрос на сервер, а сервер вытягивает необходимую информацию и отправляет ответ. В виде сервера могут выступать базы данных, сервера Apache и другие. Клиентом может выступать браузер или какой-нибудь другой вид интерфейса.

**2. Модуль аутентификации**

Система должна включать модуль аутентификации, который осуществляет проверку подлинности пользователей на основе их идентификационных данных и учетных данных.

Функции модуля:

- Проверка правильности введенных учетных данных.

- Использование безопасных методов хранения и обработки паролей.

- Поддержка различных методов аутентификации, таких как логин/пароль, двухфакторная аутентификация, биометрическая аутентификация и т.д.

**3. Модуль авторизации**

Система должна содержать модуль авторизации, который определяет права доступа пользователей к различным ресурсам и функциям системы после успешной аутентификации.

**3. Хранилище пользовательских данных**

Система должна иметь хранилище, где будут храниться данные пользователей, необходимые для аутентификации и авторизации.

Функции хранилища:

- Безопасное хранение и защита пользовательских учетных данных.

- Возможность масштабирования и управления данными пользователей.

- Поддержка механизмов шифрования для защиты конфиденциальной информации.

**4. Интерфейс пользователя**

Система должна иметь удобный и интуитивно понятный интерфейс для взаимодействия с пользователем в процессе аутентификации и авторизации.

Интерфейс должен предоставить пользователю формы для ввода и представления информации.

**5.2 Требования к процедурам доступа к системе**

**1. Процедура аутентификации**

Система должна обеспечивать процедуру аутентификации, которая гарантирует правильность идентификации пользователей перед предоставлением доступа к системе.

Функциональные требования:

- Проверка правильности введенных учетных данных (логин, пароль и т.д.).

- Возможность выбора различных методов аутентификации (логин/пароль, одноразовые пароли, биометрические данные и т.д.).

**2. Процедура авторизации**

Система должна реализовать процедуру авторизации, которая определяет права доступа пользователей к ресурсам системы после успешной аутентификации.

Функциональные требования:

- Управление ролями и группами пользователей для определения их прав доступа.

- Возможность автоматической или ручной смены ролей и прав доступа для пользователей.

**3. Процедура сброса пароля**

Система должна предоставлять процедуру сброса пароля для пользователей в случае утери или компрометации их учетных данных.

Функциональные требования:

- Возможность запроса сброса пароля через безопасные каналы связи (электронная почта, SMS и т.д.).

- Проверка подлинности пользователя при сбросе пароля для предотвращения несанкционированного доступа.

- Установка временных ограничений для нового пароля после его сброса для повышения безопасности.

**4. Процедура блокировки учетной записи**

Система должна иметь процедуру автоматической блокировки учетных записей пользователей после определенного количества неудачных попыток входа.

Функциональные требования:

- Установка параметров блокировки учетной записи (например, количество неудачных попыток и время блокировки).

- Возможность ручной разблокировки учетной записи администратором системы.

**5.3 Требования к функциональной безопасности**

**1. Проверка формата ввода пароля**

Для проверки формата пароля (минимум 8 символов, минимум 1 цифра и 1 заглавная буква) будем использовать регулярное выражение, написанное на языке Ruby:

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

Пароль, соответствующий этому регулярному выражению, будет обладать высокой степенью сложности и подходить нашим требованиям.

Фрагмент кода(?=.\*\d)отвечает за наличие хотя бы 1 цифры в пароле.

Фрагмент кода (?=.\*[a-z])отвечает за наличие хотя бы 1 прописной буквы в пароле.

Фрагмент кода (?=.\*[A-Z])отвечает за наличие хотя бы 1 заглавной буквы в пароле.

Фрагмент кода .{8, } ставит ограничение для ввода как минимум 8 символов.

**2. Защита от атак и угроз**

Система должна быть защищена от различных видов атак и угроз безопасности данных.

Функциональные требования:

- Реализация механизмов защиты от перебора паролей и других атак на учетные данные.

- Обеспечение регулярных обновлений и патчей для исправления уязвимостей безопасности системы.

**5.4 Требования к информационной безопасности**

**1. Защита конфиденциальности данных**

Система должна обеспечивать защиту конфиденциальности пользовательских данных и учетных записей.

Функциональные требования:

- Шифрование хранимых и передаваемых пользовательских данных, включая учетные данные и личную информацию.

- Установка строгих политик доступа и контроля доступа к данным на основе ролей пользователей и принципа минимальных привилегий.

**2. Резервное копирование и восстановление данных**

Система должна иметь механизмы резервного копирования и восстановления данных для обеспечения доступности информации в случае чрезвычайных ситуаций.

1. ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

**6.1 Требования к информационному обеспечению**

**1. Интеграция с внешними системами**

Система должна быть способна интегрироваться с другими информационными системами предприятия для обмена данными и обеспечения единой точки аутентификации и авторизации.

Функциональные требования:

- Реализация открытых API и стандартных протоколов для обмена данными с другими системами.

- Поддержка однократной аутентификации (Single Sign-On) для обеспечения удобства использования для пользователей.

**2. Обеспечение доступности**

- Требование: Система должна быть устойчивой к отказам и обеспечивать высокую доступность для пользователей.

**6.2 Требования к программному обеспечению**

**1. Надежность и стабильность**

Программное обеспечение должно быть надежным и стабильным, чтобы обеспечить непрерывную работу системы и минимизацию ошибок и сбоев программного обеспечения.

**2. Масштабируемость**

Программное обеспечение должно быть масштабируемым для поддержки роста числа пользователей и объема данных.

**3. Гибкость и настраиваемость**

Программное обеспечение должно быть гибким и настраиваемым для адаптации к уникальным требованиям и бизнес-процессам предприятия.

**4. Удобство использования**

Программное обеспечение должно быть удобным в использовании как для администраторов, так и для конечных пользователей.

Функциональные требования:

- Интуитивно понятный пользовательский интерфейс с простыми и понятными инструкциями.

**6.3 Требования к техническому обеспечению**

Минимальные технические требования к ЭВМ, необходимой для нормального функционирования программного обеспечения:

1) Процессор Pentium IV

2) Частота 1 Ghz

3) Оперативная память 512Mb

4) Видеокарта 128Мb

5) Клавиатура и мышь

Рекомендуемые технические требования:

1) Процессор INTEL Core 2 Quad

2) Частота 2,3 Ghz

3) Оперативная память 1Gb

4) Видеокарта 512Мb

5) Клавиатура и мышь

1. СОСТАВ И СОДЕРЖАНИЕ РАБОТ

Разработка автоматизированной системы аутентификации и авторизации на предприятии ОАО Нафтан включает в себя следующие этапы и работы:

**1. Анализ требований и сбор информации**

- Изучение потребностей и требований предприятия к системе аутентификации и авторизации.

- Сбор и анализ данных о текущих процессах аутентификации и авторизации.

- Определение функциональных и нефункциональных требований к системе.

**2. Проектирование системы**

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

- Создание диаграммы классов, взаимодействия и последовательности для описания работы системы.

- Проектирование базы данных для хранения пользовательских данных, учетных записей и прав доступа.

**3. Разработка и тестирование**

- Написание кода модулей аутентификации, авторизации и управления пользователями.

- Реализация интерфейсов пользователя для ввода учетных данных и управления доступом.

- Тестирование разработанных модулей на соответствие требованиям и обеспечение их надежной работы.

**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.

**5. Сопровождение и поддержка**

- Обеспечение технической поддержки и сопровождения системы после внедрения.

- Регулярное обновление и доработка системы в соответствии с изменяющимися требованиями и потребностями предприятия.

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

**6. Оценка эффективности**

- Проведение оценки эффективности внедренной системы с учетом достигнутых результатов и удовлетворения потребностей предприятия.

1. ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ

**1. Подготовка к приемке**

- Подготовка всех необходимых документов, включая акты о внедрении системы, техническую документацию, результаты тестирования и обучения персонала.

- Проверка готовности всех компонентов системы к эксплуатации, включая программное и аппаратное обеспечение, а также интеграцию с другими системами предприятия.

**2. Проведение приемочных испытаний**

- Проведение тестирования системы предприятием с целью проверки соответствия требованиям и качеству работы.

- Оценка функциональности системы, ее производительности, безопасности и удобства использования.

**3. Устранение замечаний и несоответствий**

- Проведение работ по устранению выявленных в ходе приемки проблем и несоответствий.

- Повторная проверка исправленных элементов системы для подтверждения их работоспособности и соответствия требованиям.

4. **Передача системы в эксплуатацию**

- Подготовка к эксплуатации системы, включая настройку оконечного оборудования, развертывание программного обеспечения и обучение пользователей.

- Передача всех необходимых доступов и прав для работы с системой соответствующим сотрудникам предприятия.

5. **Мониторинг и поддержка**

- Организация регулярного мониторинга работы системы для выявления и устранения возможных проблем и сбоев.

- Предоставление технической поддержки и консультаций пользователям системы в процессе ее эксплуатации.

1. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Требования к документированию при разработке системы аутентификации и авторизации включают в себя следующие аспекты:

**1. Техническая документация**

- Создание технической спецификации, описывающей архитектуру системы, используемые технологии, алгоритмы аутентификации и авторизации, а также методы шифрования.

- Формирование диаграмм классов, взаимодействия и последовательности для описания структуры и работы системы.

- Подготовка описания API и интерфейсов системы для интеграции с другими приложениями и сервисами.

**2. Руководства пользователя**

- Создание простого и понятного руководства, описывающего процедуры регистрации, входа в систему, восстановления пароля и управления учетной записью.

**3. Руководства администратора**

- Описание процедур управления пользователями, установки прав доступа, мониторинга безопасности и реагирования на инциденты.

**4. Тестовая документация**

- Подготовка плана тестирования, включающего в себя описание тестовых сценариев, критериев приемки и ожидаемых результатов.

- Формирование отчетов о результатах тестирования, включающих в себя описание выявленных ошибок, аномалий и рекомендации по их исправлению.

**5. Справочная информация**

- Подготовка справочной информации, включающей в себя описание основных терминов, принципов работы системы и рекомендации по ее использованию.

- Создание FAQ (часто задаваемых вопросов) для быстрого решения типичных проблем и ситуаций.

ПРИЛОЖЕНИЕ А

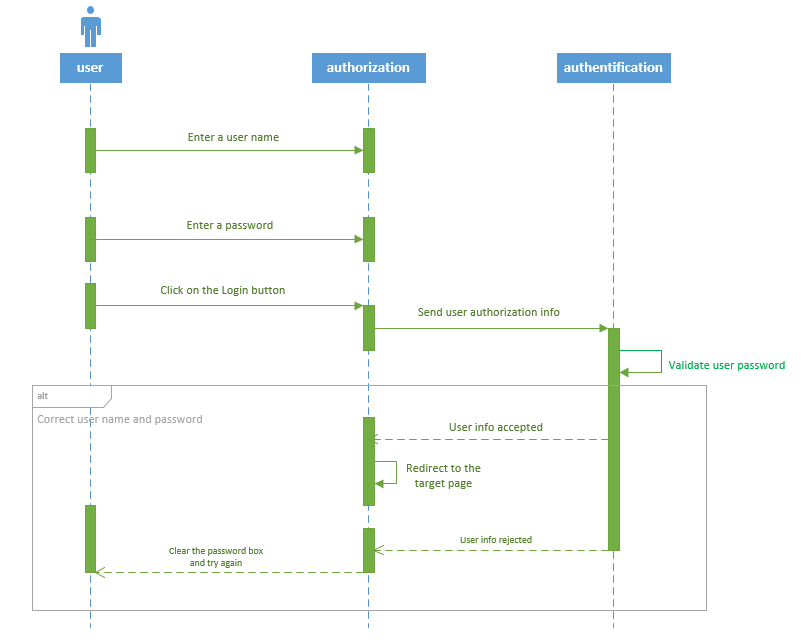


Рисунок 1 – Диаграмма последовательностей UML