**Лабораторная работа № 4**

**Разработка технических требований на создание автоматизированной системы аутентификации и автоматизации в соответствии с СТП 09150.11.118-2009**

**ОГЛАВЛЕНИЕ**

[1 ОБЩИЕ СВЕДЕНИЯ 3](#_Toc162596794)

[2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ 3](#_Toc162596795)

[3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ 3](#_Toc162596796)

[3.1 Перечень и краткая характеристика бизнес-процессов 3](#_Toc162596797)

[3.2 Требования к входным и выходным данным, формам их представления 4](#_Toc162596798)

[4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС 4](#_Toc162596799)

[4.1 Формулировка цели разработки 4](#_Toc162596800)

[4.2 Область и условия применения АС 5](#_Toc162596801)

[5 Требования к системе 5](#_Toc162596802)

[5.1 Требования к структуре 5](#_Toc162596803)

[5.2 Требования к процедурам доступа к системе 5](#_Toc162596804)

[5.3 Требования к функциональной безопасности 6](#_Toc162596805)

[5.4 Требования к информационной безопасности 6](#_Toc162596806)

[5.5 Требования к патентной чистоте 7](#_Toc162596807)

[7. Состав и содержание работ 7](#_Toc162596808)

[8. Требования к документированию 8](#_Toc162596809)

# 1 ОБЩИЕ СВЕДЕНИЯ

1.1 Наименование работы: Разработка технических требований на создание автоматизированной системы аутентификации и авторизация в соответствии с СТП 09150.11.118-2009.

1.2 Заказчик АС и Ответственный по проекту:

Заказчик АС – Учреждение образования «Белорусский государственный университет транспорта»

Ответственный по проекту – главный специалист по безопасности УО «Белорусский государственный университет транспорта»

1.3 Наименование Организации-пользователя АС: Учреждение образования «Белорусский государственный университет транспорта»

1.4 Наименование объекта внедрения: Информационно-вычислительный центр УО «Белорусский государственный университет транспорта».

# 2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

2.1 В настоящих технических требованиях применены термины и определения в следующем значении:

2.1.1 Автоматизированная система аутентификации и авторизации –­ это программное обеспечение или комплекс программных средств, которые предназначены для проверки подлинности пользователей и автоматизации процессов работы с данными или системами.

2.2 В настоящем стандарте применяют следующие сокращения:

АС – автоматизированная система;

ЕСКД – Единая система конструкторской документации;

ЕСПД – Единая система программной документации;

ППО – прикладное программное обеспечение;

ТЗ – техническое задание;

ТП – технический проект;

ЭП – эскизный проект

# 3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ

## 3.1 Перечень и краткая характеристика бизнес-процессов

3.1.1 Объектом процесса аутентификации и авторизации являются информационные системы, приложения, сервисы или другие ресурсы, к которым пользователь пытается получить доступ.

3.1.2 Предметом процесса аутентификации и авторизации является проверка личности пользователя и предоставление ему доступа к определенным ресурсам или функциям. Это включает в себя установление подлинности идентификационных данных пользователя (логин, пароль, биометрические данные) и проверку его прав на доступ к информации или функциональности.

3.1.3 Реализация автоматизированной системы аутентификации и авторизации включает взаимосвязь бизнес-процессов

1) Получение данные, введенных пользователем и проверка их

правильности ввода

2) Автоматическая загрузка персонализированных данных, настройка

рабочего пространства пользователя, автоматическое создание отчетов или выполнение других задач.

## 3.2 Требования к входным и выходным данным, формам их представления

3.2.1 Входными данными являются:

- Идентификационные данные пользователя (логин, пароль);

- Права доступа пользователя к определенным ресурсам или функциям;

- Требования к сложности пароля.

3.2.2 Выходными данными являются:

- Результат проверки подлинности пользователя (успешная или неуспешная аутентификация);

- Уровень доступа пользователя к ресурсам или функциональности.

3.2.3 Требования к данным:

- Данные должны быть защищены и передаваться по безопасным каналам связи;

- Должна быть возможность хранения и обработки большого объема данных о пользователях и их доступе;

- Должны соблюдаться законодательные требования к хранению и обработке персональных данных.

# 4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС

## 4.1 Формулировка цели разработки

Целью создания автоматизированной системы аутентификации и авторизации является:

- Обеспечение безопасного и удобного способа проверки подлинности пользователей перед предоставлением доступа к ресурсам или функциональности системы;

- Управление правами доступа пользователей в соответствии с их ролями и обязанностями;

- Оптимизация процессов аутентификации и авторизации для повышения эффективности работы пользователей и системы в целом.

## 4.2 Область и условия применения АС

АС аутентификации и авторизации предназначена для обеспечения безопасного и удобного способа проверки подлинности пользователей перед предоставлением доступа к информационным ресурсам.

# 5 Требования к системе

## 5.1 Требования к структуре

Архитектура АС должна иметь вид:

* 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

Процедура регистрации включает в себя проверку личности, создание

логина и пароля.

Пароль пользователя должен быть не менее 8 символов и обязательно содержать цифры и символы разного регистра, только латиница. 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 – 25 минут. После этого сессия уничтожается, пользователь должен вновь проходить процесс аутентификации.

## 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

Состав, структура и способы организации данных в Системе должны быть определены на этапе рабочего проектирования. Информационный обмен данными в системе должен осуществляться с помощью разработанного коммуникационного протокола передачи данных. Хранение данных в системе должно быть построено на основе современных СУБД.

Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД. Средства СУБД, а также средства используемых операционных систем должны обеспечивать документирование и протоколирование обрабатываемой в системе информации. Структура базы данных должна поддерживать кодирование хранимой и обрабатываемой информации. Доступ к данным должен быть предоставлен только авторизованным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации.

Средства СУБД, а также средства используемых операционных систем, сервера приложений и веб-сервера должны обеспечивать документирование и протоколирование.

В процессе разработки системы будет учтен тот момент, что все модули системы должны взаимодействовать друг с другом.

Информация в базе данных системы должна сохраняться при возникновении аварийных ситуаций.

Резервное копирование данных должно осуществляться на регулярной основе, в объёмах, достаточных для восстановления информации в подсистеме хранения данных.

## 6.2 Требования к математическому обеспечению

Описание и содержание алгоритмов, исполняемых в ИС, определяется в процессе разработки программного обеспечения.

## 6.3 Требования к программному обеспечению

Прикладное программное обеспечение должно отвечать следующим требованиям:

- высокая степень готовности для решения поставленных задач;

- совместимость программных продуктов в части используемых технических средств, системного ПО и общесистемной инфраструктуры в пределах требований к техническому обеспечению, а также их информационная совместимость в пределах требований к информационному обмену.

ПО должно быть разработано с учетом технологии, обеспечивать реализацию всех функций системы и решение всех поставленных задач для каждого АРМ.

ПО должно быть построено в виде программных модулей, унифицированных для каждого рабочего места.

Данные должны передаваться по сети без ущерба для функционирования всей системы.

## 6.4 Требования к техническому обеспечению

6.4.1 Основные виды технических средств:

-сервер баз данных

-рабочее место администратора БД

- сетевое оборудование

6.4.2 Минимальные характеристики технического обеспечения пользователей:

-процессор Intel Pentium III 1 Ghz

-оперативная память – 512 Mb RAM

- жесткий диск – 20 Gb HDD

## 6.5 Требования к организационному обеспечению

Организационное обеспечение АС должно быть достаточным для эффективного выполнения персоналом АС возложенных на него обязанностей при осуществлении автоматизированных и связанных с ними неавтоматизированных функций системы.

Требования к распределению обязанностей среди персонала, участвующего в функционировании АС в режиме реального времени, определяют с учетом требований организации.

# 7. Состав и содержание работ

Работы по автоматизации процесса аутентификации включают в себя следующие этапы и содержание:

1. Анализ требований: На этом этапе проводится анализ потребностей и требований к системе аутентификации. Определяются цели автоматизации, объем функциональности, требования к безопасности и удобству использования.

2. Проектирование системы: Разрабатывается архитектура системы аутентификации, определяются компоненты, взаимодействие между ними, выбираются технологии и инструменты для реализации.

3. Разработка программного обеспечения: На этом этапе создается программное обеспечение для реализации автоматизированной системы аутентификации. Разрабатываются модули для проверки подлинности пользователей, управления доступом, журналирования событий и другие необходимые функции.

4. Интеграция с существующими системами: При необходимости происходит интеграция новой системы аутентификации с уже существующими информационными системами организации. Это может включать в себя настройку API, протоколов обмена данными и других механизмов взаимодействия.

5. Тестирование и отладка: После разработки системы проводятся тесты на соответствие требованиям, исправление ошибок и устранение недочетов. Важно обеспечить надежную работу системы перед ее внедрением.

6. Внедрение и обучение пользователей: После успешного завершения тестирования система аутентификации внедряется в рабочую среду. Пользователи обучаются работе с новой системой, ознакамливаются с принципами аутентификации и правилами безопасности.

7. Сопровождение и поддержка: После внедрения системы проводится ее дальнейшее сопровождение, обновление, поддержка и мониторинг работы. В случае необходимости вносятся изменения и доработки для оптимизации процесса аутентификации.

# 8. **Требования к документированию**

В состав технической документации, разрабатываемой при доработке компонентов ИС, должны входить следующие документы:

• Спецификация;

• Текст программного кода АС;

• Инструкция по установке АС;

• Общее описание разработанной АС;

• Программа и методика испытаний разработанной АС;

• Руководство пользователя разработанной АС;

• Руководство Администратора разработанной АС. Руководство

пользователя должно содержать описание принципов и функций АС, а также способов работы на автоматизированных рабочих местах оператора.

Важно учитывать следующие требования к документированию процесса аутентификации и авторизации:

1. Полнота и точность.

Документация должна быть полной и точной, описывать все этапы процесса аутентификации, особенности реализации автоматизации, используемые технологии, алгоритмы и протоколы.

1. Ясность и понятность.

Информация в документации должна быть представлена понятным и доступным для всех участников процесса.

1. Актуальность.

Документация должна быть актуальной и соответствовать текущему состоянию системы аутентификации.

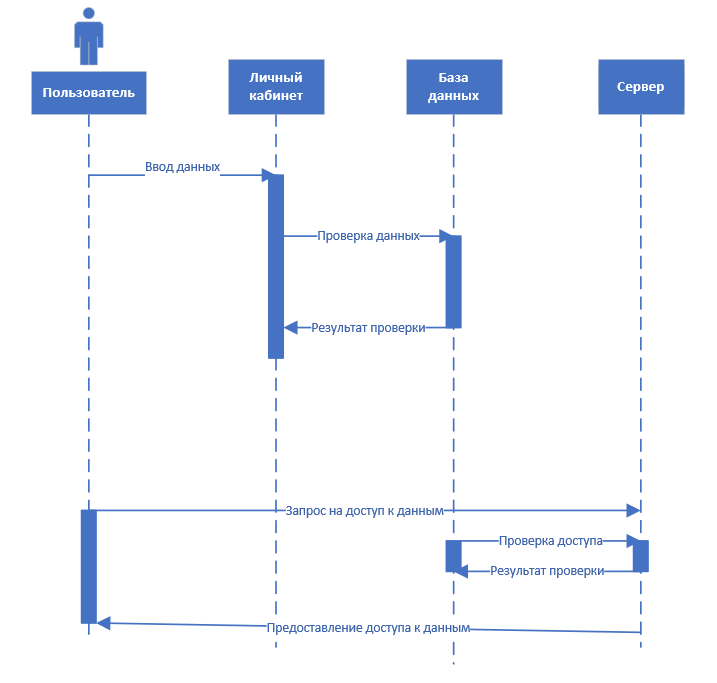
1. Безопасность.

Учитывайте меры безопасности при создании документации.

1. Доступность.

Доступ к документации должен быть обеспечен всем участникам процесса аутентификации.

**Диаграмма последовательности**

****