**ЛАБОРАТОРНАЯ РАБОТА №8**

РАЗРАБОТКА ТЕХНИЧЕСКОГО ЗАДАНИЯ НА СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ

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

**Тема проект:** разработка технического задания 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.

**Общие сведения:**

Техническое задание на разработку автоматизированной системы (ТЗ) – 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.

ТЗ является основным документом, устанавливающим требования и порядок создания автоматизированной системы, в соответствии с которым осуществляется разработка и внедрение автоматизированной системы на объекте.

Структура документа технического задания на разработку приведена в приложении А. Пример технического задания на разработку автоматизированной системы приведен в приложении Б.

**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 Общая характеристика объектов АСАА

4.2 Существующая система разработки технологической карты станции

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 по формированию базы данных

6.4 Требования к подсистеме НСИ базы данных

6.5 Требования к автоматизированному обмену данными с информационными системами

6.6 Требования к организационному обеспечению

6.7 Требования к техническому обеспечению

7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ

8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ

9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

10 ВЫВОД

# 1 **ВВЕДЕНИЕ**

Создание автоматизированных систем, особенно в области информационной безопасности, является важным аспектом для любой организации. Эти системы обеспечивают безопасность входа и использования ресурсов в соответствии с установленными правами доступа. Разработка технического задания на создание автоматизированной системы аутентификации и авторизации в соответствии с СТП 09150.11.118-2009 является ключевым этапом в этом процессе. Техническое задание устанавливает необходимые требования и параметры для создания безопасной и эффективной системы. Это имеет большое значение для обеспечения безопасности и эффективности работы организации.

# 2 ОБЩИЕ СВЕДЕНИЯ

2.1 Полное наименование: автоматизированной системы аутентификации и авторизации.

2.2 Сокращенное наименование: ТЗ АСАА.

2.3 Заказчик: ИП Козлов В.Г. 220030, г. Гомель, пр. Победы , 17;

2.4 Выполнение работ по этапам и стадиям работ, оформление и предъявление Заказчику их результатов осуществляется Исполнителем согласно требованиям данного технического задания.

# 3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ АСАА

## 3.1 Назначение АСАА

Назначением создания автоматизированной системы аутентификации и авторизации является обеспечение безопасности входа и использования ресурсов в информационных системах. Эта система предназначена для контроля доступа к информационным ресурсам и обеспечения безопасности данных, а также предотвращения несанкционированного доступа к конфиденциальной информации. Система аутентификации и авторизации позволяет ограничить доступ к информации только авторизованным пользователям, повысить уровень безопасности и защитить данные от утечек и взломов. Создание такой системы имеет важное значение для эффективного управления доступом к ресурсам и обеспечения безопасности информации в организации.

## 3.2 Цели создания АСАА

Основной целью создания автоматизированной системы аутентификации и авторизации является обеспечение безопасности информационных ресурсов и данных организации. Конкретные цели могут включать в себя:

1. Контроль доступа: Система аутентификации и авторизации предназначена для контроля доступа к информационным ресурсам и обеспечения безопасности данных. Это означает, что только авторизованные пользователи имеют доступ к информации, которая необходима для их работы.
2. Предотвращение несанкционированного доступа: Создание автоматизированной системы аутентификации и авторизации позволяет предотвратить несанкционированный доступ к конфиденциальной информации. Это достигается путем ограничения доступа к информации только тем пользователям, которые имеют соответствующие права на доступ.
3. Защита данных: Система аутентификации и авторизации также предназначена для защиты данных организации от утечек и взломов. Создание такой системы помогает предотвратить утечки конфиденциальной информации, а также защитить данные от взломов.
4. Управление доступом: Автоматизированная система аутентификации и авторизации также предназначена для эффективного управления доступом к информационным ресурсам. Создание такой системы позволяет организации установить гибкую систему прав доступа, что помогает повысить безопасность и эффективность работы организации.

# 4. ХАРАКТЕРИСТИКА ОБЪЕКТОВ АС ТЕХКАРТА И СУЩЕСТВУЮЩЕЙ СИСТЕМЫ РАЗРАБОТКИ ТЕХНОЛОГИЧЕСКОЙ КАРТЫ СТАНЦИИ

## 4.1 Общая характеристика объектов АСАА

Объектами автоматизированной системы аутентификации и авторизации являются пользователи и ресурсы, к которым пользователи должны иметь доступ.

Пользователи включают в себя всех пользователей системы, которые могут запрашивать доступ к ресурсам. Для каждого пользователя должны быть созданы учетные записи, содержащие информацию о логине, пароле и правах доступа.

Ресурсы могут включать в себя файлы, папки, базы данных, веб-сайты и другие объекты, к которым пользователи могут иметь доступ. Каждый ресурс должен быть идентифицирован и иметь установленные права доступа, которые определяют, кто может получить к нему доступ и с каким уровнем привилегий.

Система аутентификации и авторизации должна обеспечивать аутентификацию пользователей при входе в систему путем проверки их идентификатора и пароля. После успешной аутентификации система должна проверять права доступа пользователя к запрашиваемым ресурсам и разрешать или запрещать доступ в соответствии с этими правами.

Кроме того, система должна иметь механизмы управления учетными записями пользователей и правами доступа к ресурсам, а также механизмы аудита и журналирования, позволяющие отслеживать действия пользователей в системе.

Общая характеристика объектов автоматизированной системы аутентификации и авторизации заключается в том, что каждый объект должен быть идентифицирован и иметь установленные права доступа, которые должны быть контролируемы системой аутентификации и авторизации.

## 4.2 Существующая система разработки технологической карты станции

Существует множество систем разработки автоматизированных систем аутентификации и авторизации. Некоторые из них являются коммерческими продуктами, такими как Okta, Microsoft Azure Active Directory, Ping Identity и др. Другие системы, такие как OpenAM, Shibboleth, Keycloak, представляют собой свободно распространяемые решения с открытым исходным кодом.

Коммерческие системы, как правило, имеют множество дополнительных функций, таких как мультифакторная аутентификация, управление доступом на основе ролей, интеграция с другими системами и т.д. Однако, их использование может быть ограничено высокой стоимостью лицензий и зависимостью от поставщика.

Свободно распространяемые системы, наоборот, обычно имеют открытый исходный код и могут быть бесплатно использованы и модифицированы. Они также могут предоставлять ряд функций, таких как мультифакторная аутентификация, управление доступом на основе ролей и т.д. Однако, интеграция с другими системами может потребовать дополнительных усилий и опыта в области разработки.

Выбор системы разработки автоматизированной системы аутентификации и авторизации зависит от конкретных потребностей организации, ее бюджета, уровня безопасности и других факторов.

# 5 ТРЕБОВАНИЯ К АС ТЕХКАРТА

## 5.1 Требования к структуре

Структура автоматизированной системы аутентификации и авторизации должна быть построена с учетом ее целей и задач. Общая структура системы может включать в себя следующие компоненты:

1. Компонент управления аутентификацией - отвечает за процесс проверки подлинности пользователей при входе в систему и выдачу им соответствующих прав доступа. Данный компонент должен иметь механизмы защиты от несанкционированного доступа и злоупотреблений.
2. Компонент управления авторизацией - отвечает за контроль доступа к ресурсам системы, управление правами доступа и назначение ролей пользователям. Данный компонент должен обеспечивать возможность гибкой настройки прав доступа, а также механизмы защиты от нарушений конфиденциальности.
3. Компонент управления аудитом - отвечает за запись всех действий пользователей в системе, чтобы иметь возможность идентифицировать проблемы безопасности и реагировать на них. Данный компонент должен обеспечивать сохранность данных, а также гибкую настройку механизмов аудита.
4. Компонент управления сетевыми соединениями - отвечает за обеспечение безопасной работы системы в сетевой среде. Данный компонент должен обеспечивать защиту от сетевых атак и злоупотреблений, а также удобный интерфейс для настройки сетевых соединений.
5. Компонент управления безопасностью данных - отвечает за обеспечение защиты данных системы от несанкционированного доступа, изменения и уничтожения. Данный компонент должен обеспечивать защиту данных на всех этапах их жизненного цикла - от создания до уничтожения.

Все компоненты системы должны взаимодействовать между собой и обеспечивать общую безопасность системы. Кроме того, структура системы должна быть гибкой и расширяемой для возможности внесения изменений и улучшений в будущем.

## 5.2 Требования к процедурам доступа к системе.

Требования к процедурам доступа к системе, согласования и утверждения автоматизированной системы аутентификации и авторизации должны быть определены в техническом задании. Эти требования должны обеспечивать безопасность системы и защиту от несанкционированного доступа.

Процедуры доступа к системе должны определять, кто имеет право на доступ к системе, каким образом происходит идентификация пользователей, а также какие уровни доступа предоставляются в зависимости от роли пользователя в системе.

Согласование и утверждение автоматизированной системы аутентификации и авторизации должны происходить в соответствии с установленными процедурами и правилами организации. Должны быть определены процедуры согласования и утверждения документации, такие как проектная документация, техническое задание и документация на программное обеспечение.

Также важным аспектом является обеспечение безопасности при согласовании и утверждении системы. Должны быть определены механизмы защиты информации при передаче между участниками процесса, а также механизмы контроля и аудита процедур согласования и утверждения.

## 5.3 Требования к функциональной безопасности

СТП 09150.11.118-2009 устанавливает требования к функциональной безопасности автоматизированной системы аутентификации и авторизации. Ниже перечислены основные требования к функциональной безопасности автоматизированной системы аутентификации и авторизации в соответствии с данным стандартом:

1.Надежность и защищенность системы должны быть обеспечены на всех этапах ее жизненного цикла: от проектирования до эксплуатации и утилизации.

2.Система должна быть защищена от несанкционированного доступа, в том числе от атак с использованием вирусов, троянов, вредоносных программ и других средств.

3.Система должна быть способна обнаруживать попытки несанкционированного доступа и предпринимать соответствующие меры по защите от них.

4.Система должна иметь механизмы аутентификации и авторизации пользователей, а также контроля доступа к ресурсам.

5.Система должна иметь механизмы регистрации и аудита действий пользователей для обеспечения возможности расследования инцидентов и выявления несанкционированных действий.

6.Система должна иметь механизмы защиты данных, передаваемых между пользователями и системой, а также хранящихся на сервере

7.Система должна быть способна обеспечивать доступ к ресурсам только тем пользователям, которые имеют на это право.

8.Система должна обеспечивать возможность принятия мер по обеспечению безопасности, включая блокирование пользователей или установку ограничений на использование ресурсов.

9.Система должна иметь механизмы обнаружения и предотвращения атак на сервер.

10.Система должна иметь механизмы защиты от отказа в обслуживании.

## 5.4 Требования к информационной безопасности

СТП 09150.11.118-2009 устанавливает также требования к информационной безопасности автоматизированной системы аутентификации и авторизации. Ниже перечислены основные требования к информационной безопасности системы:

1.Система должна быть защищена от несанкционированного доступа к информации, передаваемой и хранимой в ней.

2.Система должна иметь механизмы шифрования данных, передаваемых между пользователями и системой, а также хранящихся на сервере.

3.Система должна иметь механизмы защиты от вирусов, троянов, вредоносных программ и других средств, направленных на нарушение информационной безопасности.

4.Система должна иметь механизмы защиты от атак на сервер, направленных на взлом системы и получение несанкционированного доступа к информации.

5.Система должна иметь механизмы контроля доступа к ресурсам, ограничивающие возможности пользователей для выполнения операций, нарушающих информационную безопасность.

6.Система должна иметь механизмы обнаружения и предотвращения атак на сервер и ресурсы системы.

7.Система должна иметь механизмы защиты от отказа в обслуживании, в том числе от DDoS-атак.

8.Система должна иметь механизмы регистрации и аудита действий пользователей для обеспечения возможности расследования инцидентов и выявления несанкционированных действий.

9.Система должна обеспечивать защиту конфиденциальной информации, передаваемой и хранящейся в ней, от несанкционированного доступа.

10.Система должна быть обеспечена надежными механизмами резервного копирования и восстановления данных в случае их потери или повреждения.

# 6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

СТП 09150.11.118-2009 устанавливает следующие требования к видам обеспечения автоматизированной системы аутентификации и авторизации:

1.Обеспечение безопасности хранения и передачи информации должно включать использование криптографических методов защиты, таких как шифрование, хэширование, электронная подпись и т.д.

2.Предусмотрение многоуровневой системы защиты информации, включающей контроль доступа, аутентификацию пользователей, контроль целостности данных, защиту от вредоносных программ, резервное копирование и восстановление данных, защиту от несанкционированного доступа и т.д.

3.Обеспечение надежности и устойчивости работы системы, включая мониторинг состояния системы, автоматическое восстановление после сбоев, обеспечение резервного питания, контроль температуры и влажности в помещении и т.д.

4.Соблюдение требований к защите персональных данных пользователей, включая обеспечение конфиденциальности и неразглашения информации о пользователях без их согласия.

5.Предусмотрение возможности аудита и мониторинга действий пользователей в системе, для выявления и предотвращения несанкционированного доступа или других нарушений безопасности.

6.Учет особенностей конкретной организации и ее требований к безопасности при выборе и использовании оборудования, программного обеспечения и технологий.

7.Соответствие требованиям и стандартам безопасности, установленным национальными и международными организациями и стандартами, таким как ISO, ГОСТ, ФЗ "О персональных данных" и т.д.

## 6.1 Требования к информационному обеспечению

СТП 09150.11.118-2009 устанавливает следующие требования к информационному обеспечению автоматизированной системы аутентификации и авторизации:

1.Система должна обеспечивать возможность аутентификации пользователей и контроля доступа к ресурсам на основе прав доступа, определенных администратором системы.

2.Обеспечение защиты от несанкционированного доступа к данным пользователей и ресурсам системы, а также контроль использования ресурсов системы.

3.Система должна обеспечивать возможность управления доступом к ресурсам системы, включая управление правами доступа и ролевым доступом.

4.Предусмотрение защиты данных, передаваемых между компонентами системы, включая шифрование и цифровую подпись.

5.Обеспечение механизмов контроля и мониторинга действий пользователей в системе, включая возможность аудита и журналирования.

6.Предусмотрение механизмов автоматической блокировки доступа при обнаружении несанкционированного доступа или других нарушений безопасности.

7.Система должна обеспечивать возможность анализа и обработки журналов аудита, для выявления и предотвращения нарушений безопасности.

8.Обеспечение надежности и устойчивости работы системы, включая возможность резервного копирования и восстановления данных, контроль целостности данных и т.д.

9.Система должна соответствовать требованиям законодательства и стандартам безопасности, включая обеспечение конфиденциальности и защиты персональных данных.

10.Система должна обеспечивать возможность управления пользователями, включая возможность регистрации новых пользователей, изменения прав доступа и ролей, а также удаление пользователей.

## 6.2 Требования к программному обеспечению

СТП 09150.11.118-2009 устанавливает следующие требования к программному обеспечению автоматизированной системы аутентификации и авторизации:

1.Надежность и стабильность работы программного обеспечения, включая обеспечение защиты от ошибок и сбоев.

2.Совместимость программного обеспечения с другими системами и устройствами, используемыми в комплексе с автоматизированной системой аутентификации и авторизации.

3.Обеспечение безопасности данных, в том числе шифрования данных и защиты от несанкционированного доступа.

4.Гибкость настройки и конфигурирования программного обеспечения для удовлетворения требований пользователя.

5.Оптимальное использование ресурсов компьютерной системы, в том числе минимизация потребления ресурсов и оптимизация производительности.

6.Поддержка многоязычности и возможность локализации программного обеспечения для использования в различных странах и регионах.

7.Удобство использования и интерфейс пользователя, который понятен и интуитивно понятен для всех пользователей системы.

8.Возможность масштабирования системы для увеличения ее мощности и расширения функциональности.

9.Поддержка резервного копирования и восстановления данных, чтобы обеспечить сохранность данных при возникновении непредвиденных ситуаций.

10.Регулярные обновления и патчи программного обеспечения для устранения уязвимостей и обеспечения безопасности системы.

## 6.3 Требования по формированию базы данных

СТП 09150.11.118-2009 устанавливает следующие требования по формированию базы данных автоматизированной системы аутентификации и авторизации:

1. Безопасность и защита данных: База данных должна обеспечивать защиту информации и безопасность доступа к данным, включая защиту от несанкционированного доступа, изменений и уничтожения данных. Доступ к базе данных должен быть предоставлен только уполномоченным лицам.
2. Контроль доступа: База данных должна поддерживать гибкие механизмы контроля доступа, обеспечивая доступ только для авторизованных пользователей.
3. Интеграция с другими системами: База данных должна поддерживать интеграцию с другими информационными системами, используемыми в комплексе с автоматизированной системой аутентификации и авторизации.
4. Полнота и точность данных: База данных должна содержать полную и точную информацию о пользователях и их правах доступа к ресурсам системы.
5. Структура и организация данных: База данных должна быть хорошо структурирована и организована для обеспечения эффективной работы системы и быстрого доступа к данным.
6. Гибкость и масштабируемость: База данных должна обеспечивать гибкость и масштабируемость для возможности добавления новых пользователей и ресурсов системы.
7. Резервное копирование и восстановление: База данных должна поддерживать резервное копирование и восстановление данных, чтобы обеспечить сохранность данных при возникновении непредвиденных ситуаций.
8. Аудит и журналирование: База данных должна поддерживать аудит и журналирование, чтобы обеспечить возможность отслеживания действий пользователей и обнаружения нарушений безопасности.
9. Поддержка многоязычности: База данных должна поддерживать многоязычность для использования в различных странах и регионах.
10. Соответствие международным стандартам: База данных должна соответствовать международным стандартам безопасности данных и быть совместимой с другими системами безопасности данных.

## 6.4 Требования к подсистеме НСИ базы данных

СТП 09150.11.118-2009 - это стандарт технического задания на разработку программных средств. В соответствии с ним, требования к подсистеме НСИ базы данных автоматизированной системы аутентификации и авторизации должны включать следующие пункты:

Надежность и безопасность: подсистема НСИ должна быть защищена от несанкционированного доступа и взлома. Необходимо предусмотреть механизмы аутентификации и авторизации пользователей, а также контроль доступа к данным. Подсистема должна иметь механизмы резервного копирования и восстановления данных.

Гибкость и масштабируемость: подсистема НСИ должна поддерживать изменения в структуре данных и масштабироваться при увеличении объема информации. Должны быть предусмотрены механизмы оптимизации производительности при работе с большими объемами данных.

Эффективность: подсистема НСИ должна обеспечивать быстрый доступ к данным, особенно при больших объемах информации. Необходимо предусмотреть оптимизацию запросов и механизмы кэширования данных.

Удобство использования: подсистема НСИ должна иметь простой и удобный интерфейс для работы с данными. Интерфейс должен быть интуитивно понятным и позволять быстро находить необходимые данные.

Соответствие стандартам: подсистема НСИ должна соответствовать стандартам безопасности и качества, установленным для баз данных. Необходимо предусмотреть соблюдение стандартов по защите персональных данных.

Возможность интеграции: подсистема НСИ должна интегрироваться с другими подсистемами автоматизированной системы аутентификации и авторизации, а также с другими информационными системами. Должны быть предусмотрены механизмы обмена данными между системами.

Гибкость настройки: администраторы должны иметь возможность настраивать параметры работы подсистемы НСИ в соответствии с требованиями системы. Необходимо предусмотреть механизмы конфигурирования и настройки системы.

Возможность анализа данных: подсистема НСИ должна предоставлять возможность анализировать данные и получать статистические отчеты. Для этого необходимо предусмотреть механизмы формирования отчетов и аналитических запросов.

Совместимость: подсистема НСИ должна быть совместима с различными базами данных и операционными системами. Должны быть предусмотрены механизмы обеспечения совместимости с различными платформами.

Документирование: необходимо вести документацию на подсистему НСИ базы данных, в которой должны быть описаны ее функциональные и технические характеристики, требования к системе и документация по установке, настройке и эксплуатации системы.

## 6.5 Требования к автоматизированному обмену данными с информационными системами

Требования к автоматизированному обмену данными с информационными системами в рамках автоматизированной системы аутентификации и авторизации включают:

1. Обмен данными: автоматизированная система аутентификации и авторизации должна обеспечивать возможность автоматизированного обмена данными с информационными системами, в том числе с внешними системами. Для этого необходимо определить структуру данных и форматы обмена данными.

2. Интерфейсы: необходимо определить типы и характеристики интерфейсов, которые будут использоваться для автоматизированного обмена данными с информационными системами. Интерфейсы могут быть реализованы с помощью протоколов передачи данных, веб-сервисов, API и других технологий.

3. Скорость и производительность: необходимо обеспечить быстрый и эффективный обмен данными между информационными системами. Для этого необходимо оптимизировать процессы обмена данными, а также предусмотреть возможность распределения нагрузки на несколько серверов.

4. Безопасность: автоматизированный обмен данными должен быть безопасным и защищенным от несанкционированного доступа. Для этого необходимо использовать современные методы шифрования и аутентификации, а также контролировать доступ к информации.

5. Мониторинг и логирование: необходимо обеспечить мониторинг и логирование процесса автоматизированного обмена данными. Это поможет выявить ошибки и проблемы, а также обеспечит возможность анализа производительности системы.

6. Обработка ошибок: необходимо предусмотреть механизмы обработки ошибок, которые могут возникнуть в процессе автоматизированного обмена данными. Это поможет предотвратить потерю данных и обеспечить корректную работу системы.

7. Тестирование: необходимо проводить тестирование процесса автоматизированного обмена данными, чтобы убедиться в его корректной работе. Тестирование должно включать в себя проверку функциональности, производительности, безопасности и мониторинга.

8. Совместимость: необходимо обеспечить совместимость процесса автоматизированного обмена данными с другими информационными системами и технологиями. Для этого необходимо учитывать стандарты и протоколы, используемые в других системах.

9. Резервное копирование и восстановление: необходимо обеспечить возможность резервного копирования и восстановления данных, которые передаются в рамках процесса автоматизированного обмена данными. Это поможет предотвратить потерю данных в случае сбоев в системе.

10. Управление версиями: необходимо предусмотреть механизмы управления версиями данных, которые передаются в рамках процесса автоматизированного обмена данными. Это позволит контролировать изменения в данных и обеспечить их согласованность между информационными системами.

11. Масштабируемость: необходимо предусмотреть возможность масштабирования процесса автоматизированного обмена данными при увеличении объема данных или количества информационных систем, которые участвуют в процессе.

12. Автоматизация: процесс автоматизированного обмена данными должен быть максимально автоматизирован, чтобы минимизировать вмешательство человека и уменьшить вероятность ошибок.

13. Система мониторинга: необходимо создать систему мониторинга процесса автоматизированного обмена данными, которая будет контролировать его работу и предупреждать о возможных сбоях или проблемах.

14. Конфигурационное управление: необходимо проводить конфигурационное управление процессом автоматизированного обмена данными, чтобы контролировать изменения в конфигурации и обеспечить ее согласованность с требованиями системы.

## 6.6 Требования к организационному обеспечению

Организационное обеспечение автоматизированной системы аутентификации и авторизации включает в себя следующие требования, установленные СТП 09150.11.118-2009:

1. Определение ролей и прав доступа: необходимо определить роли пользователей и установить соответствующие им права доступа к информационным ресурсам. Это поможет обеспечить безопасность и защиту данных от несанкционированного доступа.

2. Обеспечение безопасности информации: необходимо обеспечить безопасность информации, которая обрабатывается и хранится в автоматизированной системе аутентификации и авторизации. Для этого необходимо использовать современные методы шифрования, аутентификации и контроля целостности данных.

3. Обучение пользователей: необходимо обучать пользователей автоматизированной системы аутентификации и авторизации. Пользователи должны быть проинформированы о правилах безопасности и процедурах аутентификации и авторизации.

4. Организация управления доступом: необходимо организовать управление доступом к информационным ресурсам и контроль доступа пользователей. Для этого необходимо использовать систему управления доступом, которая позволит определять права доступа и контролировать их выполнение.

5. Обеспечение защиты от внешних угроз: необходимо обеспечить защиту от внешних угроз, таких как хакерские атаки и вирусы. Для этого необходимо использовать современные антивирусные программы и фаерволы.

6. Обеспечение конфиденциальности: необходимо обеспечить конфиденциальность информации, которая передается через автоматизированную систему аутентификации и авторизации. Для этого необходимо использовать средства шифрования данных.

7. Система резервного копирования: необходимо создать систему резервного копирования данных автоматизированной системы аутентификации и авторизации, чтобы обеспечить возможность быстрого восстановления данных в случае их потери.

8. Организация аудита: необходимо организовать аудит использования автоматизированной системы аутентификации и авторизации. Аудит позволит контролировать использование системы и выявлять несанкционированный доступ и другие нарушения.

## 6.7 Требования к техническому обеспечению

СТП 09150.11.118-2009 устанавливает следующие требования к техническому обеспечению автоматизированной системы аутентификации и авторизации:

1. Система должна обеспечивать надежную и безопасную работу при обработке информации, включая защиту от несанкционированного доступа и использования, а также обеспечивать сохранность информации.

2. Оборудование, на котором работает система, должно соответствовать требованиям безопасности и качества, а также рекомендациям производителей программных средств.

3. Система должна поддерживать работу в условиях высоких нагрузок, а также обеспечивать быстрый и надежный доступ к информации.

4. Система должна иметь средства мониторинга, обеспечивающие контроль за состоянием и работой оборудования и программного обеспечения, а также предупреждение о возможных сбоях или проблемах.

5. Для обеспечения безопасности работы системы должны использоваться средства защиты информации, включая аппаратные и программные средства шифрования, контроля целостности информации, аутентификации и авторизации пользователей.

6. Система должна обеспечивать возможность резервного копирования и восстановления информации в случае сбоя оборудования или программного обеспечения.

7. При проектировании системы должны учитываться требования к масштабируемости и расширяемости, чтобы обеспечить возможность добавления новых функций и компонентов в будущем.

8. Система должна обеспечивать совместимость с другими информационными системами, с которыми необходимо осуществлять обмен данными.

9. Система должна обеспечивать возможность удаленного управления и мониторинга, а также управления доступом пользователей.

# 7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ

7.1 Состав, содержание и этапность выполнения работ определяются согласно календарному плану к договору.

7.2 Заказчик организует поставку необходимого оборудования и лицензионного программного обеспечения.

7.3 Состав и перечень документов, предъявляемых по окончании соответствующих стадий и этапов, определяется в соответствии с договором на разработку АСАА.

7.4 Основные этапы разработки выполняются в соответствии с нормативными документами.

# 8 ПОРЯДОК ПРИЕМКИ АСАА В ЭКСПЛУАТАЦИЮ

8.1 Приемо-сдаточные испытания разработанного программного продукта и документации по каждому этапу разработки АСАА осуществляются комиссией в соответствии с календарным планом к договору.

8.2 На технических ресурсах Белорусской железной дороги проводится опытная эксплуатация АСАА. Затем Заказчиком должен быть решен вопрос о порядке и сроках внедрения и вводе АСАА в промышленную эксплуатацию.

8.3 Результаты этапов работ по их завершению оформляются двухсторонним актом Заказчика и Исполнителя.

8.4 По завершению разработки Исполнитель представляет документацию по АСАА и проводит обучение администраторов и пользователей отделений Белорусской железной дороги.

# 9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

9.1 Вся разрабатываемая документация оформляется в соответствии с действующими нормативными документами.

9.2 К АСАА должна прилагаться инструкция пользователю. Рабочая документация должна соответствовать действующим стандартам и ГОСТ, ЕСКД и ЕСПД.

**10 ВЫВОД**

Таким образом, разработка технического задания на создание автоматизированной системы аутентификации и авторизации в соответствии с СТП 09150.11.118-2009 включает в себя определение целей и задач системы, описание требований к функциональным и нефункциональным характеристикам системы, а также требования к техническому, организационному и информационному обеспечению.

Одним из ключевых аспектов разработки такого технического задания является обеспечение безопасности и защиты информации, обрабатываемой системой, в том числе защита от несанкционированного доступа, шифрование, контроль целостности информации и аутентификация пользователей.

Кроме того, важно учитывать требования к техническому обеспечению системы, такие как надежность и быстродействие, масштабируемость и совместимость с другими информационными системами.

Разработка технического задания на создание автоматизированной системы аутентификации и авторизации в соответствии с СТП 09150.11.118-2009 требует высокой квалификации разработчиков и должна проводиться в соответствии с определенными процедурами и методиками, чтобы обеспечить качественный результат.