СОДЕРЖАНИЕ

[Введение 2](#_Toc132641920)

[2 Общие сведения 2](#_Toc132641921)

[3 Назначение и цели создания 2](#_Toc132641922)

[3.1 Назначение 2](#_Toc132641923)

[3.2 Цели создания 2](#_Toc132641924)

[4 Характеристика объектов системы разработки 2](#_Toc132641925)

[5 Требования к системе 3](#_Toc132641926)

[5.1 Требования к структуре 3](#_Toc132641927)

[5.2 Требования к процедурам доступа к системе 3](#_Toc132641928)

[5.3 Требования к функциональной безопасности 3](#_Toc132641929)

[5.4 Требования к информационной безопасности 3](#_Toc132641930)

[5.5 Требования к патентной чистоте 3](#_Toc132641931)

[6 Требования к видам обеспечения 4](#_Toc132641932)

[6.1. Требования к информационному обеспечению 4](#_Toc132641933)

[6.2. Требования к математическому обеспечению 4](#_Toc132641934)

[6.3. Требования к программному обеспечению 4](#_Toc132641935)

[6.4. Требования к техническому обеспечению 4](#_Toc132641936)

[СОСТАВ И СОДЕРЖАНИЕ РАБОТ 4](#_Toc132641937)

[ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ 5](#_Toc132641938)

[ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ 5](#_Toc132641939)

[9.1. Общие требования 5](#_Toc132641940)

[9.2. Требования к составу документации 5](#_Toc132641941)

[9.3. Требования к содержанию документации 6](#_Toc132641942)

# Введение

Целью данного технического задания является описание требований к разработке автоматизированной системы аутентификации и авторизации в соответствии с требованиями СТП 09150.11.118-2009.

Автоматизированная система аутентификации и авторизации предназначена для обеспечения безопасного доступа пользователей к информационным ресурсам организации. Она должна обеспечивать аутентификацию пользователей, контроль доступа и управление правами доступа в соответствии с установленными правилами и политиками безопасности.

В данном техническом задании будут описаны требования к структуре системы, ее функциональным возможностям, требованиям к безопасности, а также требования к обеспечению.

# 2 Общие сведения

Наименование системы: Автоматизированная система аутентификации и авторизации (далее – Система). Назначение системы: Система предназначена для обеспечения контроля доступа к защищенным ресурсам, а также для авторизации пользователей в информационных системах.

Основные функции системы:

* Аутентификация пользователей;
* Авторизация пользователей;
* Управление правами доступа пользователей;
* Журналирование действий пользователей;
* Обеспечение информационной безопасности.
* В состав Системы входят:
* Сервер аутентификации и авторизации;
* Клиентские приложения для аутентификации и авторизации;
* Административный интерфейс для управления правами доступа пользователей;
* Журналы аутентификации и авторизации.

# 3 Назначение и цели создания

## 3.1 Назначение

Назначением системы является обеспечение безопасности доступа к информационным ресурсам организации путем проверки подлинности пользователей и предоставления им прав доступа в соответствии с уровнем их полномочий.

## 3.2 Цели создания

Основной целью создания системы является повышение уровня безопасности доступа к информационным ресурсам организации, улучшение контроля за доступом пользователей и уменьшение риска несанкционированного доступа.

# 4 Характеристика объектов системы разработки

Система разработки должна включать в себя следующие объекты:

* сервер аутентификации и авторизации
* клиентское приложение для взаимодействия с сервером
* база данных пользователей и их прав доступа
* средства для защиты информации, передаваемой между клиентским приложением и сервером
* средства для резервного копирования и восстановления данных

# 5 Требования к системе

## 5.1 Требования к структуре

Система должна быть построена на клиент-серверной архитектуре с использованием протоколов HTTPS и SSL для обеспечения безопасности передачи данных. Клиентское приложение должно быть написано на языке программирования, обеспечивающем быстродействие и совместимость с различными операционными системами.

## 5.2 Требования к процедурам доступа к системе

Доступ к системе должен быть осуществлен только после аутентификации пользователя и проверки его прав доступа. Для аутентификации и авторизации пользователей должны использоваться протоколы безопасной передачи данных, такие как SSL или TLS.

## 5.3 Требования к функциональной безопасности

Система должна обеспечивать защиту от несанкционированного доступа к информации и функционалу системы. Для этого должны быть реализованы следующие меры безопасности:

Шифрование данных, передаваемых между клиентским и серверным модулями

Ограничение прав доступа пользователей на основе их ролей и привилегий

Защита паролей пользователей от несанкционированного доступа

Логирование всех операций, связанных с аутентификацией и авторизацией пользователей

## 5.4 Требования к информационной безопасности

Система должна обеспечивать защиту от несанкционированного доступа к конфиденциальной информации пользователей, хранящейся в базе данных системы. Для этого должны быть реализованы следующие меры безопасности:

Шифрование данных, хранящихся в базе данных системы

Резервное копирование данных системы для обеспечения их сохранности в случае сбоя системы

## 5.5 Требования к патентной чистоте

В процессе разработки системы необходимо обеспечить патентную чистоту. Для этого должны быть произведены все необходимые проверки на наличие патентных прав и лицензий на используемые компоненты и технологии.

# 6 Требования к видам обеспечения

## 6.1. Требования к информационному обеспечению

1 Система должна поддерживать работу с операционными системами Windows, Linux, MacOS. 6

2 Система должна иметь возможность работы с базами данных MySQL, PostgreSQL, Oracle.

3 Система должна обеспечивать интеграцию с Active Directory.

## 6.2. Требования к математическому обеспечению

Система должна обеспечивать расчет криптографических функций SHA256 и SHA512. 6.2.2 Система должна обеспечивать проверку цифровой подписи.

## 6.3. Требования к программному обеспечению

1 Система должна быть написана на языке программирования Java.

2 Система должна использовать Spring Framework для реализации основных функций.

3 Система должна использовать Hibernate для работы с базами данных.

4 Система должна использовать Apache Tomcat в качестве сервера приложений.

## 6.4. Требования к техническому обеспечению

1 Система должна работать на серверах с конфигурацией не менее Intel Xeon E5-2620 v4, 16 ГБ оперативной памяти, жестких дисках RAID 1, скорость интерфейса 1 Гбит/с.

2 Система должна использовать сетевое оборудование сети 1 Гбит/с, включая коммутаторы и маршрутизаторы.

3 Система должна обеспечивать резервное копирование данных на отдельном сервере с хранением не менее 14 дней.

# СОСТАВ И СОДЕРЖАНИЕ РАБОТ

1. Разработка технического проекта

Изучение требований и основных положений СТП 09150.11.118-2009.

Разработка архитектуры системы аутентификации и авторизации.

Разработка технического проекта автоматизированной системы аутентификации и авторизации.

Подготовка технической документации.

2. Разработка программного обеспечения

Разработка программного модуля аутентификации.

Разработка программного модуля авторизации.

Интеграция программных модулей.

3. Разработка информационного обеспечения

Разработка базы данных для хранения информации о пользователях и правах доступа.

Разработка программного обеспечения для обеспечения целостности и конфиденциальности информации.

4. Разработка математического обеспечения

Разработка алгоритмов аутентификации и авторизации.

5. Разработка технического обеспечения

Подбор необходимого оборудования.

Установка и настройка оборудования.

6. Организационное обеспечение

Планирование и организация работ.

Подготовка кадров для работы с системой аутентификации и авторизации

Проведение тестирования системы.

7. Внедрение и сопровождение

Установка и внедрение системы на объекте заказчика.

Проведение обучения пользователей системы.

Поддержка и сопровождение системы.

# ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ

Порядок приема в эксплуатацию автоматизированной системы аутентификации и авторизации должен быть следующим:

1. После окончания разработки и тестирования системы, необходимо провести ее предварительное внедрение в тестовой среде.
2. В процессе тестирования необходимо проверить работоспособность системы в различных режимах, а также ее соответствие требованиям, указанным в техническом задании.
3. По результатам тестирования необходимо разработать акт о приемке системы в эксплуатацию, в котором должны быть указаны все выявленные недостатки и требования к их устранению.
4. После устранения всех выявленных недостатков, необходимо провести повторное тестирование системы, после чего составить акт окончательной приемки системы в эксплуатацию.
5. После окончательной приемки системы в эксплуатацию, необходимо провести инструктаж пользователей, а также обеспечить техническую поддержку и сопровождение системы в процессе ее эксплуатации.

# ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

## 9.1. Общие требования

1. Все этапы разработки системы, включая этапы проектирования, тестирования и внедрения, должны быть документированы.

2. Документация должна соответствовать нормативным требованиям, установленным для разработки информационных систем.

3. Вся документация должна быть предоставлена заказчику в электронном виде на съемном носителе информации (CD, DVD или USB-накопитель).

## 9.2. Требования к составу документации

Состав документации должен включать следующие разделы:

1) техническое задание на разработку системы;

2) технический проект;

3) рабочая документация, включающая описание системы, инструкции по установке, настройке и эксплуатации, инструкции по обслуживанию и ремонту;

4) тестовая документация;

5) акты на приемку системы заказчиком.

Документация должна быть оформлена в соответствии с требованиями государственных стандартов и нормативных документов.

Все документы должны иметь уникальный номер и дату выпуска.

## 9.3. Требования к содержанию документации

Техническое задание на разработку системы должно содержать следующую информацию:

1) наименование системы;

2) цели и задачи создания системы;

3) требования к системе, в том числе функциональные и нефункциональные требования;

4) описание пользователей системы и их ролей;

5) описание процессов, реализуемых в системе;

6) требования к безопасности системы;

7) требования к документированию;

8) требования к тестированию системы.

Технический проект должен содержать следующую информацию:

1) общее описание системы;

2) структуру системы и описание ее компонентов;

3) описание интерфейсов и протоколов взаимодействия компонентов;

4) описание алгоритмов и процедур системы;

5) требования к надежности и доступности системы;

6) требования к производительности системы;

7) требования к поддержке и обслуживанию системы;

8) требования к документированию;

9) требования к защите информации;