Управление Белорусской железной дороги  
(наименование объекта автоматизации)

3  
(класс автоматизированной системы)

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ  
К РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ  
АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ(АСАА)**

На 12 листах

**ПРИЛОЖЕНИЕ А**

(справочное)

Структура документа технических требований на разработку

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 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА

**1 ВВЕДЕНИЕ**

Автоматизированная система аутентификации и авторизации представляет собой программный комплекс, предназначенный для обеспечения безопасного доступа пользователей к информационным ресурсам организации. В условиях постоянного роста киберугроз и ужесточения требований к защите данных создание надежной системы управления доступом становится критически важной задачей для любой компании, работающей с конфиденциальной информацией.

Настоящее техническое задание разработано в соответствии с требованиями стандарта СТП 09150.11.118-2009 и определяет основные принципы, цели и технические требования к создаваемой системе. Документ содержит полное описание функциональных возможностей системы, требований к безопасности, техническому и программному обеспечению, а также порядок внедрения и приемки системы в эксплуатацию.

Разрабатываемая система предназначена для интеграции в существующую информационную инфраструктуру организации и будет использоваться для контроля доступа сотрудников, партнеров и клиентов к защищенным ресурсам. Основными функциями системы станут аутентификация пользователей, авторизация доступа к ресурсам, ведение журналов безопасности и защита от несанкционированных действий.

**2 ОБЩИЕ СВЕДЕНИЯ**

Разрабатываемая автоматизированная система аутентификации и авторизации представляет собой комплекс программных модулей, обеспечивающих безопасный доступ пользователей к информационным ресурсам организации. Система предназначена для использования в корпоративных информационных системах, государственных учреждениях и других организациях, где требуется надежный контроль доступа к данным.

Основными компонентами системы являются модуль аутентификации, модуль авторизации, модуль управления учетными записями и модуль аудита. Модуль аутентификации отвечает за проверку подлинности пользователей при помощи различных методов, включая традиционные логин и пароль, двухфакторную аутентификацию и биометрические данные. Модуль авторизации определяет уровень доступа пользователя к тем или иным ресурсам на основе назначенных ролей или индивидуальных прав.

Модуль управления учетными записями предоставляет администраторам системы возможность создавать, редактировать и блокировать учетные записи пользователей, назначать им соответствующие права доступа. Модуль аудита ведет журнал всех событий, связанных с доступом к системе, фиксируя успешные и неудачные попытки входа, изменения прав доступа и другие значимые действия.

Технологической основой системы станут современные языки программирования, такие как Python, Java или C#, и надежные системы управления базами данных, включая PostgreSQL и Microsoft SQL Server. Для обеспечения безопасности передаваемых данных будет использоваться протокол TLS версии 1.3, а для хранения паролей - современные алгоритмы хеширования.

Система может быть реализована в различных архитектурных вариантах в зависимости от потребностей заказчика. Для небольших организаций может быть достаточно монолитной архитектуры, тогда как крупные предприятия могут потребовать микросервисного подхода или гибридной модели, сочетающей локальные и облачные компоненты.

Важным аспектом разработки является соответствие системы международным и отраслевым стандартам информационной безопасности. Система будет разрабатываться с учетом требований ГОСТ Р ИСО/МЭК 27001, а при использовании в финансовом секторе - стандарта PCI DSS.

Среди ограничений системы можно отметить отсутствие поддержки устаревших протоколов аутентификации, что является осознанным решением для обеспечения максимального уровня безопасности. Также система потребует регулярного обновления для защиты от новых видов киберугроз.

Перспективы развития системы включают возможность интеграции с биометрическими системами аутентификации, внедрение механизмов анализа поведения пользователей для выявления аномальной активности, а также использование технологий распределенного реестра для дополнительного уровня защиты.

Внедрение автоматизированной системы аутентификации и авторизации позволит организации значительно повысить уровень защиты своих информационных ресурсов, минимизировать риски утечки конфиденциальных данных и обеспечить соответствие требованиям регуляторов в области информационной безопасности.

**3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ**

3.1 Назначение

Автоматизированная система аутентификации и авторизации (АСАА) предназначена для обеспечения безопасного и контролируемого доступа пользователей к информационным ресурсам организации. Основное назначение системы заключается в реализации механизмов проверки подлинности пользователей (аутентификации) и определения их прав доступа к различным ресурсам (авторизации).

Система выполняет несколько ключевых функций:

- Идентификация и аутентификация пользователей при входе в систему

- Контроль и разграничение прав доступа к данным и функциональным возможностям

- Защита от несанкционированного доступа к конфиденциальной информации

- Фиксация и учет всех действий пользователей в системе

- Обеспечение соответствия требованиям информационной безопасности

АСАА предназначена для использования в различных типах организаций:

- В коммерческих компаниях для защиты корпоративных данных

- В государственных учреждениях для обеспечения безопасности информации

- В финансовых организациях для защиты персональных данных клиентов

- В медицинских учреждениях для контроля доступа к медицинским записям

Система может быть интегрирована с различными информационными системами организации, включая:

- Корпоративные порталы и ERP-системы

- Системы электронного документооборота

- CRM-системы и базы данных клиентов

- Специализированные отраслевые решения

3.2 Цели создания

Основные цели создания автоматизированной системы аутентификации и авторизации можно разделить на несколько ключевых направлений:

1. Обеспечение информационной безопасности

- Защита конфиденциальных данных от несанкционированного доступа

- Предотвращение утечки информации

- Обеспечение конфиденциальности, целостности и доступности данных

- Соответствие требованиям законодательства в области защиты информации

2. Оптимизация процессов управления доступом

- Централизованное управление правами доступа пользователей

- Упрощение процедур предоставления и отзыва прав

- Автоматизация процессов назначения и изменения ролей

- Снижение нагрузки на ИТ-персонал при управлении доступом

3. Повышение эффективности работы

- Минимизация времени на процедуры аутентификации

- Обеспечение бесперебойного доступа авторизованных пользователей

- Снижение количества ошибок при назначении прав доступа

- Ускорение процессов адаптации новых сотрудников

4. Обеспечение подотчетности и аудита

- Фиксация всех действий пользователей в системе

- Возможность анализа событий безопасности

- Формирование отчетов о деятельности пользователей

- Обеспечение доказательной базы при расследовании инцидентов

5. Поддержка бизнес-процессов организации

- Обеспечение безопасного удаленного доступа сотрудников

- Поддержка различных сценариев работы с системой

- Интеграция с другими корпоративными системами

- Масштабируемость под изменяющиеся потребности бизнеса

Для достижения этих целей система должна реализовывать следующие функциональные возможности:

- Поддержка различных методов аутентификации (парольная, многофакторная, биометрическая)

- Гибкая система назначения прав доступа (ролевая модель, атрибутивная модель)

- Возможность тонкой настройки политик безопасности

- Механизмы принудительного изменения паролей

- Блокировка учетных записей при подозрительной активности

- Формирование детализированных журналов событий

- Генерация отчетов по активности пользователей

Система должна обеспечивать высокий уровень безопасности при сохранении удобства использования для конечных пользователей. Важным аспектом является баланс между строгими мерами безопасности и производительностью системы, чтобы не создавать излишних затруднений в работе авторизованных пользователей.

Реализация системы аутентификации и авторизации позволит организации:

- Значительно снизить риски информационной безопасности

- Соответствовать требованиям регуляторов и стандартов

- Оптимизировать процессы управления доступом

- Повысить эффективность работы сотрудников

- Получить инструменты для анализа и аудита действий пользователей

Достижение этих целей будет способствовать общему повышению уровня информационной безопасности организации и созданию надежной основы для защиты критически важных данных и бизнес-процессов.

**4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ**

Автоматизированная система аутентификации и авторизации взаимодействует с несколькими ключевыми объектами, каждый из которых играет важную роль в обеспечении безопасности и функциональности системы. Основными объектами системы являются:

Пользователи системы - физические лица, которым предоставляется доступ к информационным ресурсам. Пользователи делятся на три основные категории: администраторы безопасности, операторы системы и обычные пользователи. Администраторы обладают максимальными правами и отвечают за настройку системы, управление учетными записями и мониторинг событий безопасности. Операторы осуществляют техническое обслуживание системы и обработку запросов пользователей. Обычные пользователи работают в системе в рамках предоставленных им полномочий.

Учетные записи пользователей содержат идентификационные данные и параметры доступа для каждого зарегистрированного в системе пользователя. Каждая учетная запись включает уникальный идентификатор, аутентификационные данные (логин, хеш пароля, биометрические шаблоны), информацию о пользователе (ФИО, должность, контактные данные), а также флаги состояния (активна/заблокирована/истек срок действия).

Роли и права доступа определяют перечень разрешенных действий для каждой категории пользователей. Система использует ролевую модель управления доступом (RBAC), где права группируются по функциональным ролям. Для каждой роли определяется набор разрешений на доступ к конкретным ресурсам и операциям. Роли могут наследовать права друг от друга, образуя иерархическую структуру.

Журналы безопасности фиксируют все значимые события в системе, включая успешные и неудачные попытки аутентификации, изменения прав доступа, модификацию учетных записей и другие действия, влияющие на безопасность системы. Каждая запись журнала содержит временную метку, идентификатор пользователя, тип события, его результат и дополнительную контекстную информацию.

**5 ТРЕБОВАНИЯ К СИСТЕМЕ**

5.1 Требования к структуре

Система должна иметь модульную архитектуру, состоящую из следующих основных компонентов:

Ядро системы обеспечивает базовую функциональность и взаимодействие между модулями. Оно отвечает за загрузку конфигурации, управление сессиями пользователей, обработку системных событий и обеспечение работы API для интеграции с другими системами.

Модуль аутентификации реализует механизмы проверки подлинности пользователей. Он должен поддерживать несколько методов аутентификации: по логину и паролю, с использованием одноразовых кодов (SMS, email), аппаратных токенов и биометрических данных. Для парольной аутентификации требуется реализовать политику сложности паролей, включая минимальную длину, использование разных категорий символов и запрет повторного использования последних паролей.

Модуль авторизации управляет правами доступа пользователей к ресурсам системы. Он должен реализовывать ролевую модель управления доступом с возможностью определения сложных правил доступа на основе атрибутов пользователя, времени суток, местоположения и других параметров. Модуль должен кэшировать решения о доступе для повышения производительности.

Модуль аудита отвечает за регистрацию событий безопасности и генерацию отчетов. Он должен фиксировать все значимые действия пользователей и системные события, обеспечивая целостность и защиту журналов от модификации. Для хранения журналов должна использоваться отдельная защищенная база данных с возможностью архивирования и ротации записей.

5.2 Требования к процедурам доступа к системе

Процедура аутентификации должна включать следующие этапы:

1. Идентификация пользователя по уникальному логину

2. Проверка подлинности с использованием выбранного метода аутентификации

3. Проверка состояния учетной записи (активность, срок действия)

4. Создание сессии с уникальным идентификатором

5. Запись события в журнал аудита

Для административного доступа должна быть реализована многофакторная аутентификация с обязательным использованием как минимум двух независимых факторов (например, пароль + одноразовый код). Система должна блокировать учетную запись после 5 неудачных попыток входа на период не менее 30 минут. При попытках подбора паролей с разных IP-адресов система должна активировать дополнительные механизмы защиты.

5.3 Требования к функциональной безопасности

Система должна обеспечивать:

- Шифрование всех передаваемых данных с использованием протокола TLS 1.2 или выше

- Хранение паролей в виде криптографических хешей с использованием современных алгоритмов (bcrypt, Argon2)

- Защиту от атак типа "человек посередине" и replay-атак

- Регулярную смену криптографических ключей

- Контроль целостности исполняемых файлов и конфигураций

5.4 Требования к информационной безопасности

Система должна соответствовать:

- ГОСТ Р ИСО/МЭК 27001 - требования к системам управления информационной безопасностью

- ГОСТ Р 57580.1 - требования к защите персональных данных

- PCI DSS (для финансовых организаций)

- Требованиям регуляторов отрасли

Должны быть реализованы механизмы защиты от:

- SQL-инъекций и других видов инъекционных атак

- Межсайтового скриптинга (XSS)

- Подделки межсайтовых запросов (CSRF)

- Переполнения буфера

- Атак на сессии пользователей

5.5 Требования к патентной чистоте

Система должна использовать только лицензионное программное обеспечение и алгоритмы, не нарушающие патентных прав третьих лиц. Все криптографические алгоритмы должны быть стандартизированы и не подпадать под действие патентных ограничений. В случае использования открытого ПО необходимо соблюдать требования соответствующих лицензий (GPL, MIT, Apache).

**6 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА**

6.1 Сроки выполнения проекта определяются согласно календарному плану к договору на разработку автоматизированной системы аутентификации и авторизации (АСАА). Общая продолжительность работ не должна превышать 12 месяцев с момента заключения договора.

6.2 Основные этапы разработки выполняются в следующей последовательности и сроки:

- Анализ требований и проектирование архитектуры - 2 месяца

- Разработка основных модулей системы - 4 месяца

- Тестирование компонентов системы - 2 месяца

- Интеграция с инфраструктурой заказчика - 2 месяца

- Опытная эксплуатация - 1 месяц

- Ввод в промышленную эксплуатацию - 1 месяц

6.3 Приемо-сдаточные испытания разработанного программного продукта и документации по каждому этапу разработки АСАА осуществляются комиссией в составе представителей заказчика и исполнителя в соответствии с календарным планом к договору. Испытания проводятся по заранее согласованным методикам.

6.4 На технических ресурсах заказчика проводится опытная эксплуатация АСАА продолжительностью не менее 30 календарных дней. По результатам опытной эксплуатации заказчиком принимается решение о порядке и сроках ввода системы в промышленную эксплуатацию.

6.5 Результаты каждого этапа работ по их завершению оформляются двухсторонним актом заказчика и исполнителя. Акт должен содержать перечень выполненных работ, достигнутые результаты и выявленные замечания (при наличии).

6.6 По завершению разработки исполнитель представляет полный комплект документации на АСАА, включая:

- Техническое описание системы

- Руководство администратора

- Руководство пользователя

- Программную документацию

И проводит обучение администраторов и пользователей системы.

6.7 Настоящие технические требования могут уточняться и корректироваться по взаимной договоренности между заказчиком и исполнителем в рабочем порядке. Все изменения оформляются дополнительными соглашениями к договору.

6.8 В случае необходимости внесения существенных изменений в техническое задание, влияющих на сроки выполнения работ, стороны согласовывают новый календарный план реализации проекта

