Управление Белорусской железной дороги

(наименование объекта автоматизации)

3

(класс автоматизированной системы)

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ**

**К РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ**

**АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ**

На 17 листах

**Содержание**

[1. ОБЩИЕ ТРЕБОВАНИЯ 3](#_Toc194065974)

[2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ 3](#_Toc194065975)

[3. ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ 4](#_Toc194065976)

[4. ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС 6](#_Toc194065977)

[5. ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС 7](#_Toc194065978)

[6. СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА 9](#_Toc194065979)

# ОБЩИЕ ТРЕБОВАНИЯ

1.1 Наименование работы: разработка технических требований на автоматизированную систему аутентификации и авторизации (АС АА).

1.2 Заказчик АС и Ответственный по проекту: заказчик АС – Организация А;

Ответственный по проекту – информационно-технический отдел Организации А.

1.3 Наименование Организации-пользователя АС: Организация А.

1.4 Наименование объекта внедрения: информационная инфраструктура Организации А.

# 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 (АС АА) – программно-аппаратный комплекс, обеспечивающий идентификацию пользователей, проверку их прав доступа и контроль за безопасностью работы в информационной системе.

2.1.2 Аутентификация – процесс проверки подлинности пользователя на основе предоставленных учетных данных (пароль, биометрические данные, токен и др.).

2.1.3 Авторизация – процесс предоставления или ограничения прав доступа пользователя к определенным ресурсам системы после успешной аутентификации.

2.1.4 Роль пользователя – совокупность прав и ограничений, определяющая уровень доступа к функционалу системы.

2.1.5 Многофакторная аутентификация (MFA) – метод проверки подлинности, использующий два и более независимых фактора (пароль, SMS-код, биометрия и др.).

2.1.6 Токен аутентификации – уникальный идентификатор, генерируемый системой и используемый для подтверждения личности пользователя без повторного ввода учетных данных.

2.1.7 Журнал безопасности – системный лог, фиксирующий события, связанные с входами, попытками доступа, изменениями прав пользователей и другими действиями, влияющими на безопасность.

2.1.8 LDAP (Lightweight Directory Access Protocol) – сетевой протокол, используемый для работы с каталогами пользователей и управления учетными записями.

2.1.9 Резервное копирование – процесс создания копий данных, обеспечивающий их сохранность и восстановление в случае сбоя или утраты.

2.1.10 Остальные термины и определения применены в значениях, указанных в действующей нормативно-технической документации.

2.2 В настоящих технических требованиях использованы сокращения:

АС – автоматизированная система;

АС АА – автоматизированная система аутентификации и авторизации;

API – программный интерфейс приложения;

IAM – управление идентификацией и доступом (Identity and Access Management);

LDAP – протокол доступа к каталогам (Lightweight Directory Access Protocol);

MFA – многофакторная аутентификация (Multi-Factor Authentication);

RBAC – управление доступом на основе ролей (Role-Based Access Control);

SSO – единый вход в систему (Single Sign-On);

ПО – программное обеспечение;

БД – база данных.

# ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ

#### 3.1 Перечень и краткая характеристика бизнес-процессов

3.1.1 Объектом автоматизации является процесс управления доступом к информационным ресурсам Организации А с применением механизмов аутентификации и авторизации.

3.1.2 Управление доступом в Организации А осуществляется на трех уровнях:

* корпоративном: обеспечение централизованного контроля доступа к ключевым системам и сервисам;
* подразделенческом: разграничение прав доступа сотрудников различных отделов и департаментов;
* индивидуальном: персонализированное управление доступом на основе ролей и политик безопасности.

3.1.3 Предметом автоматизации является процесс аутентификации и авторизации пользователей в корпоративной информационной системе, включающий в себя идентификацию пользователей, проверку прав доступа и контроль действий в защищенной среде.

3.1.4 АС АА включает автоматизацию трех взаимосвязанных бизнес-процессов:

* управление учетными записями пользователей;
* контроль и мониторинг доступа;
* администрирование политик безопасности.

3.1.5 Управление учетными записями пользователей включает в себя:

* регистрацию и удаление учетных записей;
* управление ролями и правами пользователей;
* интеграцию с внешними каталогами пользователей.

3.1.6 Контроль и мониторинг доступа включает в себя:

* ведение журнала аутентификации и авторизации;
* анализ событий безопасности;
* уведомление администраторов о подозрительных действиях.

3.1.7 Администрирование политик безопасности включает в себя:

* настройку правил доступа к системам и сервисам;
* управление сроками действия учетных записей и паролей;
* контроль соответствия требованиям информационной безопасности.

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

3.2.1 Входными данными для работы АС АА являются:

* учетные записи пользователей и их атрибуты;
* данные об уровнях доступа и ролях пользователей;
* политики безопасности и правила аутентификации;
* логи входов и действий пользователей;
* данные о текущем состоянии учетных записей (активность, блокировки, сроки действия).

3.2.2 Выходными данными АС АА являются:

* результаты аутентификации и авторизации;
* отчеты о входах пользователей и попытках доступа;
* данные о нарушениях политики безопасности;
* уведомления о несанкционированных попытках доступа;
* аналитические отчеты по управлению доступом.

3.2.3 Входные и выходные данные должны представляться в формате, обеспечивающем:

* возможность идентификации пользователей и их прав доступа;
* структурированное хранение информации в БД и логах системы;
* возможность экспорта данных для интеграции с другими системами.

3.2.4 Формой представления выходных данных являются:

* журналы аутентификации и авторизации (табличный вид);
* графические отчеты и диаграммы о входах и активности пользователей;
* текстовые уведомления и предупреждения о нарушениях безопасности.

Таблица 3.1 – Формат представления выходных данных

|  |  |
| --- | --- |
| **Наименование параметра** | **Формат представления** |
| Идентификатор пользователя | Текст (до 50 знаков) |
| Время аутентификации | Дата/время |
| Результат аутентификации | Текст (успех/ошибка) |
| Уровень доступа пользователя | Текст (до 30 знаков) |
| Источник запроса аутентификации | IP-адрес (xxx.xxx.xxx.xxx) |
| Попытки входа за период | Число (до 3 знаков) |

3.2.5 Источниками получения входных данных являются:

* корпоративная база учетных записей пользователей;
* внешние системы каталогов (LDAP, Active Directory);
* системы мониторинга безопасности;
* базы данных журналов событий.

3.2.6 Источники получения входных данных для АС АА приведены в таблице 3.2.

Таблица 3.2 – Источники получения входных данных

|  |  |
| --- | --- |
| **Наименование параметра** | **Источник информации** |
| Учетные записи пользователей | База данных учетных записей |
| Политики безопасности | Конфигурация АС АА |
| Логи аутентификации | Система мониторинга безопасности |
| Данные об уровнях доступа | Active Directory, LDAP |
| Попытки входа и активности | Журналы событий ОС и приложений |

#### 3.3 Выполняемые технологические операции

Автоматизации подлежат технологические операции:

* управление учетными записями пользователей, включая регистрацию, удаление и обновление учетных данных;
* процесс аутентификации пользователей, включая проверку учетных данных и факторов аутентификации;
* процесс авторизации пользователей, определение уровня доступа на основе политик безопасности;
* ведение и анализ журналов событий, включая логирование попыток входа, успешных и неудачных аутентификаций;
* мониторинг подозрительных действий и автоматическое реагирование на возможные инциденты безопасности;
* генерация отчетов по активности пользователей и анализу доступа.

# ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС

#### 4.1 Формулировка цели разработки

Целями создания АС АА являются:

* автоматизация процесса аутентификации и авторизации пользователей;
* контроль и управление доступом в корпоративной среде;
* минимизация человеческого фактора в процессе администрирования;
* соответствие требованиям регуляторов;
* отказоустойчивость и защита от атак;
* масштабируемость и адаптивность под будущие изменения в политике безопасности и архитектуре сети.

#### 4.2 Область и условия применения АС

АС АА предназначена для использования в Организации А в целях обеспечения информационной безопасности и управления доступом.

#### 4.3 Ограничения применения АС

АС должна функционировать на корпоративных серверах и рабочих станциях сотрудников, соответствующих требованиям ИБ.

#### 4.4 Требования к надежности и масштабируемости

АС должна обеспечивать высокую отказоустойчивость, возможность горизонтального масштабирования и быстрого восстановления после сбоев.

# ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС

#### 5.1 Требования к АС в целом

АС ЭПР должна разрабатываться на платформе Web-технологий по принципу «сервер – тонкий клиент» с учетом адаптации под локальное программное обеспечение Белорусской железной дороги.

Клиентский доступ к АС ЭПР обеспечивается посредством интернет-браузера. Доступ к АС ЭПР из других информационных систем обеспечивается через программный интерфейс API.

#### 5.1.2 Требования к защите информации от несанкционированного доступа

АС АА должна обеспечивать многоуровневую защиту данных, включая авторизацию, шифрование данных, защиту от атак и аудит безопасности.

#### 5.1.3 Требования по сохранности информации при авариях

АС АА должна предусматривать механизмы резервного копирования, восстановления данных и защиты от критических отказов системы.

#### 5.1.4 Требования к информационному обеспечению

5.1.4.1 Информационное обеспечение АС АА представляет собой совокупность данных, необходимых для функционирования системы. Оно должно включать учетные записи пользователей, политики безопасности, логи аутентификации и авторизации, а также данные о правах доступа.

5.1.4.2 Информационная структура должна обеспечивать целостность, актуальность и доступность данных, а также их защиту от несанкционированного изменения.

5.1.4.3 Ввод и корректировка информации должны осуществляться администраторами с последующим автоматизированным контролем изменений и аудитом действий пользователей.

5.1.4.4 Поиск, извлечение и обновление данных должны быть оптимизированы для обеспечения высокой скорости работы АС АА без потери надежности и безопасности.

#### 5.1.5 Требования к математическому обеспечению

5.1.5.1 Математическое обеспечение АС АА включает алгоритмы аутентификации, обработки логов, анализа событий безопасности и принятия решений о предоставлении или блокировке доступа.

5.1.5.2 Алгоритмы должны быть адаптивными, масштабируемыми и настраиваемыми в зависимости от политики безопасности организации.

5.1.5.3 Математическое обеспечение должно учитывать возможность интеграции с внешними системами анализа угроз и предотвращения атак.

#### 5.1.6 Требования к программному обеспечению

5.1.6.1 АС АА должна разрабатываться с использованием актуальных технологий и соответствовать стандартам безопасности.

5.1.6.2 Программное обеспечение должно обеспечивать бесперебойную работу системы, устойчивость к сбоям и атакам, а также соответствовать требованиям производительности.

5.1.6.3 В системе должны быть реализованы механизмы логирования, самодиагностики и автоматического обновления компонентов.

5.1.6.4 ПО АС АА должно быть кроссплатформенным и поддерживать работу в различных средах без потери функциональности.

#### 5.1.7 Требования к организационному обеспечению

5.1.7.1 Организационное обеспечение АС АА должно предусматривать регламенты работы с системой, порядок администрирования и мониторинга ее состояния.

5.1.7.2 Сопровождение и эксплуатация системы должны осуществляться назначенными администраторами безопасности.

5.1.7.3 Должны быть предусмотрены процедуры обучения пользователей и администраторов работе с системой, а также регулярные проверки на соответствие политике безопасности.

#### 5.1.8 Требования к патентной чистоте

5.1.8.1 При выполнении работ Исполнителем обеспечивается патентная чистота результатов работ. Данная работа не должна содержать патентов, зарегистрированных в Республике Беларусь и других странах.

5.1.8.2 По требованию Заказчика Исполнитель представляет сведения о рыночной стоимости созданных при выполнении работ объектов интеллектуальной собственности.

#### 5.1.9 Требования к документированию

5.1.9.1 Вся документация на АС АА оформляется в соответствии с действующими нормативными документами.

#### 5.1.10 Требования к масштабируемости

5.1.10.1 АС АА должна поддерживать возможность увеличения количества пользователей и нагрузок без ухудшения производительности.

5.1.10.2 Архитектура системы должна предусматривать горизонтальное и вертикальное масштабирование.

#### 5.1.11 Требования к интеграции

5.1.11.1 АС АА должна обеспечивать взаимодействие с внешними системами каталогов (LDAP, Active Directory) и поддерживать стандарты OAuth, SAML.

5.1.11.2 Интеграция с корпоративными сервисами должна быть реализована через API с безопасным протоколом обмена данными.

#### 5.2 Требования к функциям (задачам), выполняемым подсистемами

#### 5.2.1 Подсистема «Управление учетными записями» предназначена для:

* регистрации, изменения и удаления учетных записей пользователей;
* управления ролями и правами доступа пользователей;
* синхронизации данных с внешними каталогами (LDAP, Active Directory).

#### 5.2.2 Подсистема «Контроль и мониторинг доступа» выполняет задачи:

* ведения журналов аутентификации и авторизации;
* анализа событий безопасности и выявления аномалий;
* уведомления администраторов о подозрительных действиях.

#### 5.2.3 Подсистема «Администрирование политик безопасности» включает в себя:

* настройку и управление политиками безопасности;
* контроль сроков действия учетных записей и паролей;
* аудит соответствия требованиям информационной безопасности.

#### 5.2.4 Подсистема «Формирование отчетности» обеспечивает:

* генерацию отчетов по активности пользователей;
* экспорт данных в различные форматы (PDF, CSV, XLSX);
* визуализацию аналитической информации (диаграммы, графики).

# СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА

6.1 Внедрение АС АА осуществляется поэтапно в соответствии с планом-графиком, утвержденным Заказчиком, и включает в себя подготовку инфраструктуры, развертывание системы, тестирование, обучение персонала и ввод в эксплуатацию.

6.2 Основные этапы внедрения:

* установка и настройка оборудования и программного обеспечения;
* интеграция с внешними системами и базами данных;
* тестирование функциональности и безопасности системы;
* обучение администраторов и конечных пользователей;
* опытная эксплуатация и корректировка системы;
* промышленная эксплуатация с мониторингом работы.

6.3 Приемо-сдаточные испытания проводятся комиссией, состоящей из представителей Заказчика, Исполнителя и ключевых пользователей, и включают тестирование на соответствие техническим требованиям, анализ производительности и оценку надежности системы.

6.4 Опытная эксплуатация проводится на ограниченном сегменте информационной инфраструктуры Организации А в течение периода, установленного Заказчиком.

6.5 По результатам опытной эксплуатации Исполнитель вносит необходимые корректировки, после чего принимается решение о переводе системы в промышленную эксплуатацию.

6.6 Промышленная эксплуатация АС АА включает:

* мониторинг работы системы в реальном времени;
* контроль за безопасностью и соответствием политик доступа;
* проведение регламентных работ по обновлению и оптимизации;
* обработку и анализ инцидентов, связанных с аутентификацией и авторизацией.

6.7 По завершении внедрения Исполнитель передает Заказчику полный комплект документации, включая:

* руководство пользователя;
* техническое описание системы;
* инструкции по администрированию и эксплуатации;
* регламентные процедуры обновления и резервного копирования.

6.8 Исполнитель проводит обучение администраторов, специалистов по безопасности и конечных пользователей, обеспечивая их необходимыми знаниями для эффективной работы с системой.

6.9 В течение гарантийного периода Исполнитель оказывает техническую поддержку, включая исправление выявленных ошибок, консультирование пользователей и обновление системы.

**НАСТОЯЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ МОГУТ УТОЧНЯТЬСЯ И КОРРЕКТИРОВАТЬСЯ ПО ВЗАИМНОЙ ДОГОВОРЕННОСТИ МЕЖДУ ЗАКАЗЧИКОМ И ИСПОЛНИТЕЛЕМ В РАБОЧЕМ ПОРЯДКЕ.**