Управление Белорусской железной дороги

(наименование объекта автоматизации)

3

(класс автоматизированной системы)

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ**

**К РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЕЙ (АС ААП)**

На 17 листах

# ОГЛАВЛЕНИЕ

1. [ОБЩИЕ СВЕДЕНИЯ 6](#_bookmark0)
2. [ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ 6](#_bookmark1)
3. [ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ 7](#_bookmark2)
   1. [Перечень и краткая характеристика бизнес-процессов 7](#_bookmark3)
   2. [Требования к входным и выходным данным, формам их представления 9](#_bookmark4)
   3. [Выполняемые технологические операции 11](#_bookmark5)
4. [ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС 11](#_bookmark6)
   1. [Формулировка цели разработки 11](#_bookmark7)
   2. [Область и условия применения АС 11](#_bookmark8)
   3. [Ограничения применения АС 11](#_bookmark9)
5. [ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС 12](#_bookmark10)
   1. [Требования к АС в целом 12](#_bookmark11)
      1. [Требования к структуре и функционированию АС 12](#_bookmark12)

[5 1.2 Требования к защите информации от несанкционированного доступа12](#_bookmark13)

* + 1. [Требования по сохранности информации при авариях 13](#_bookmark14)
    2. [Требования к информационному обеспечению 13](#_bookmark15)
    3. [Требования к математическому обеспечению 14](#_bookmark16)
    4. [Требования к программному обеспечению 14](#_bookmark17)
    5. [Требования к организационному обеспечению 14](#_bookmark18)
    6. [Требования к патентной чистоте 15](#_bookmark19)
    7. [Требования к документированию 15](#_bookmark20)
  1. [Требования к функциям (задачам), выполняемым подсистемами 15](#_bookmark21)

1. [СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА 16](#_bookmark22)

# ОБЩИЕ СВЕДЕНИЯ

* 1. Наименование работы: Разработка технических требований на автоматизированную систему аутентификации и авторизации пользователей (АС ААП).
  2. Заказчик АС и Ответственный по проекту: заказчик АС – Государственное объединение «Белорусская железная дорога; Ответственный по проекту – служба технической политики и инвестиций Государственного объединения «Белорусская железная дорога».
  3. Наименование Организации-пользователя АС: Государственное объединение «Белорусская железная дорога.
  4. Наименование объекта внедрения: Управление Белорусской железной дороги.

# ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

* 1. В настоящих технических требованиях применены термины и определения в следующем значении:
     1. **Автоматизированная система аутентификации и авторизации (АС ААП)** – программно-аппаратный комплекс, предназначенный для идентификации пользователей, проверки их прав доступа и управления сессиями на сайте.
     2. **Аутентификация** – процесс проверки подлинности пользователя путем подтверждения его учетных данных (логина и пароля).
     3. **Авторизация** – процесс предоставления пользователю прав доступа к определенным ресурсам или функциям сайта на основе его роли или уровня доступа.
     4. **Пользователь** – физическое или юридическое лицо, зарегистрированное в системе и имеющее учетную запись для доступа к ресурсам сайта.
     5. **Учетная запись** – набор данных, уникально идентифицирующих пользователя в системе, включая логин, пароль и другие атрибуты (например, электронная почта, роль, уровень доступа).
     6. **Сессия** – период взаимодействия пользователя с системой, начинающийся после успешной аутентификации и заканчивающийся после выхода пользователя или истечения времени бездействия.
     7. **Шифрование** – процесс преобразования данных в форму, недоступную для прочтения без использования специального ключа, с целью защиты конфиденциальной информации.
     8. **Роль пользователя** – набор прав и разрешений, определяющих уровень доступа пользователя к ресурсам и функциям сайта.
     9. **Остальные термины и определения** применены в значениях, указанных в действующей нормативно-технической документации, регулирующей разработку и эксплуатацию информационных систем.
  2. В настоящих технических требованиях использованы сокращения:

**АС ААП** – автоматизированная система аутентификации и авторизации пользователей;

**API** – интерфейс программирования приложений (Application Programming Interface);

**БД** – база данных;

**ИБ** – информационная безопасность;

**ЛК** – личный кабинет пользователя;

**ПО** – программное обеспечение;

**СУБД** – система управления базами данных;

**UML** – унифицированный язык моделирования (Unified Modeling Language);

**HTTPS** – защищенный протокол передачи гипертекста (HyperText Transfer Protocol Secure).

# ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ

## Перечень и краткая характеристика бизнес-процессов

* + 1. Объектом автоматизации является система аутентификации и авторизации пользователей на сайте, обеспечивающая безопасный доступ к ресурсам и управление учетными записями.
    2. Процесс аутентификации и авторизации на сайте осуществляется на следующих уровнях:
* **Уровень пользователя:** взаимодействие пользователя с системой через веб-интерфейс (ввод логина и пароля, восстановление доступа, смена пароля).
* **Уровень приложения:** обработка запросов пользователя, проверка учетных данных, управление сессиями и правами доступа.
* **Уровень безопасности:** шифрование данных, защита от несанкционированного доступа, обеспечение конфиденциальности и целостности информации.
  + 1. Предметом автоматизации является процесс управления доступом пользователей к ресурсам сайта, включающий:
* Аутентификацию пользователей путем проверки их учетных данных (логин и пароль).
* Авторизацию пользователей на основе их ролей и прав доступа.
* Управление сессиями пользователей (создание, поддержание и завершение сессий).
* Восстановление доступа к учетным записям в случае утери пароля.
  + 1. Процесс аутентификации и авторизации включает следующие этапы:
* Ввод пользователем логина и пароля.
* Проверка корректности введенных данных на стороне сервера.
* Создание сессии пользователя при успешной аутентификации.
* Предоставление доступа к ресурсам сайта в соответствии с ролью пользователя.
* Завершение сессии при выходе пользователя из системы или истечении времени бездействия.

3.1.5 Реализация автоматизированной системы аутентификации и авторизации (АС ААП) включает автоматизацию следующих бизнес-процессов:

* Регистрация пользователей: создание учетных записей, проверка уникальности логина, шифрование паролей.
* Аутентификация пользователей: проверка учетных данных, создание и управление сессиями.
* Авторизация пользователей: определение прав доступа на основе ролей пользователей.
* Восстановление доступа: сброс и восстановление пароля через подтверждение по электронной почте или другим способом.
* Управление учетными записями: редактирование профиля пользователя, смена пароля, блокировка учетных записей.

3.1.6 Формирование исходных данных для системы включает:

* Создание базы данных для хранения учетных записей пользователей.
* Настройка ролей и прав доступа для различных категорий пользователей.
* Интеграция с другими системами (например, CRM, ERP) для обмена данными о пользователях.

3.1.7 Процесс аутентификации и авторизации осуществляется за счет реализации следующих задач:

* Проверка корректности логина и пароля.
* Шифрование и хранение паролей в защищенном виде.
* Управление сессиями пользователей (время жизни сессии, автоматическое завершение при бездействии).
* Проверка прав доступа пользователя к запрашиваемым ресурсам.

3.1.8 Процесс восстановления доступа включает:

* Генерацию временного пароля или ссылки для восстановления.
* Отправку уведомления пользователю на электронную почту или мобильное устройство.
* Проверку и подтверждение данных для восстановления доступа.

3.1.9 Обязательным условием функционирования АС ААП является обеспечение безопасности данных пользователей, включая:

* Шифрование паролей и других конфиденциальных данных.
* Защиту от атак, таких как brute force, SQL-инъекции и XSS.
* Своевременное завершение сессий при отсутствии активности пользователя (не более 10 минут).

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

**3.2.1 Входными данными для системы аутентификации и авторизации (АС ААП) являются:**

* **Учетные данные пользователя:**
  + Логин (уникальный идентификатор пользователя, например, электронная почта или имя пользователя).
  + Пароль (строка символов, соответствующая требованиям безопасности: не менее 8 символов, включая цифры, буквы разного регистра и специальные символы).
* **Дополнительные данные пользователя (опционально):**
  + Электронная почта.
  + Номер телефона.
  + Роль пользователя (например, администратор, модератор, обычный пользователь).
* **Данные для восстановления доступа:**
  + Электронная почта или номер телефона для отправки кода подтверждения.
* **Данные о сессии:**
  + IP-адрес пользователя.
  + Устройство и браузер пользователя.
  + Время начала и окончания сессии.

**3.2.2 Выходными данными АС ААП являются:**

* **Результат аутентификации:**
  + Успешная аутентификация (доступ к системе предоставлен).
  + Ошибка аутентификации (неверный логин или пароль, учетная запись заблокирована и т.д.).
* **Данные о сессии:**
  + Уникальный идентификатор сессии (токен).
  + Время жизни сессии.
* **Данные о правах доступа:**
  + Список доступных ресурсов и функций в зависимости от роли пользователя.
* **Результат восстановления доступа:**
  + Временный пароль или ссылка для сброса пароля.
  + Подтверждение успешного восстановления доступа.

**3.2.3 Входные и выходные данные должны представляться в форме, позволяющей средствами автоматизации:**

* Их идентифицировать (уникальные идентификаторы для пользователей, сессий и ролей).
* Обрабатывать их (например, проверка корректности пароля, шифрование данных).
* Хранить их в защищенном виде (шифрование паролей, использование HTTPS для передачи данных).

**3.2.4 Форма представления выходных данных:**

* **Результат аутентификации:**
  + JSON-объект, содержащий статус аутентификации и данные о сессии.  
    Пример:

json

Copy

{

"status": "success",

"session\_id": "abc123",

"user\_role": "admin",

"expires\_in": 3600

}

* **Ошибка аутентификации:**  
  Пример:

json

Copy

{

"status": "error",

"message": "Invalid username or password"

}

* **Данные для восстановления доступа:**  
  Пример:

json

Copy

{

"status": "success",

"reset\_token": "xyz456",

"expires\_in": 600

}

**3.2.5 Форма представления промежуточных данных:**

* **График активности пользователей:**
  + График, отображающий количество активных сессий за определенный период времени.  
    Пример:

plaintext

Copy

Активные сессии за последние 24 часа:

12:00 - 50

13:00 - 60

14:00 - 55

**3.2.6 Источники получения входных данных:**

* **Пользовательский ввод:**
  + Логин и пароль, вводимые пользователем на форме входа.
  + Данные для восстановления доступа, вводимые пользователем на форме восстановления пароля.
* **База данных пользователей:**
  + Учетные записи пользователей, включая логины, зашифрованные пароли, роли и контактные данные.
* **Системные данные:**
  + IP-адрес, устройство и браузер пользователя, определяемые автоматически.

**3.2.7 Источники получения входных данных (параметров) для системы аутентификации и авторизации приведены в таблице 3.2.**

**Таблица 3.2 – Источники получения входных данных (параметров)**

| **Наименование параметра** | **Источник данных** |
| --- | --- |
| Логин пользователя | Ввод пользователя на форме входа |
| Пароль пользователя | Ввод пользователя на форме входа |
| Электронная почта | База данных пользователей |
| Номер телефона | База данных пользователей |
| Роль пользователя | База данных пользователей |
| IP-адрес и данные устройства | Автоматическое определение системой |
| Время начала и окончания сессии | Система управления сессиями |

## Выполняемые технологические операции

Автоматизации подлежат следующие технологические операции:

**1. Формирование исходных данных:**

* Идентификация пользователя: проверка уникальности логина и корректности введенных данных при регистрации.
* Верификация учетных данных: проверка логина и пароля при аутентификации.
* Получение дополнительных данных: сбор информации о роли пользователя, IP-адресе, устройстве и браузере для создания сессии.

**2. Проведение аутентификации и авторизации:**

* Проверка учетных данных: сравнение введенного пароля с зашифрованным паролем, хранящимся в базе данных.
* Создание сессии: генерация уникального идентификатора сессии (токена) и установка времени жизни сессии.
* Проверка прав доступа: определение доступных ресурсов и функций на основе роли пользователя.

**3. Управление сессиями:**

* Контроль активности пользователя: автоматическое завершение сессии при отсутствии активности в течение заданного времени (например, 10 минут).
* Защита от несанкционированного доступа: блокировка сессии при обнаружении подозрительной активности (например, попытки входа с разных IP-адресов).

**4. Восстановление доступа:**

* Генерация временного пароля или ссылки для сброса пароля.
* Отправка уведомления пользователю на электронную почту или мобильное устройство.
* Проверка и подтверждение данных для восстановления доступа.

**5. Формирование выходных данных:**

* Результат аутентификации: предоставление доступа к системе или сообщение об ошибке.
* Данные о сессии: возврат уникального идентификатора сессии и времени ее жизни.
* Данные о правах доступа: предоставление списка доступных ресурсов и функций в зависимости от роли пользователя.

**6. Логирование и мониторинг:**

* Запись событий: фиксация всех попыток входа, успешных и неудачных аутентификаций, изменений в учетных записях.
* Мониторинг активности: отслеживание количества активных сессий, времени их начала и окончания.

# ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС

## Формулировка цели разработки

**Целью работы** является разработка автоматизированной системы аутентификации и авторизации пользователей (АСАА), обеспечивающей:

1. **Единый и безопасный доступ** к ресурсам за счет создания интегрированной системы управления доступом.
2. **Повышение уровня защиты данных** путем внедрения современных методов шифрования и механизмов противодействия несанкционированному доступу.
3. **Автоматизацию процессов** входа, управления правами доступа и восстановления учетных записей для снижения временных затрат пользователей и администраторов.
4. **Точное и надежное управление доступом** на основе ролевой модели (RBAC) с учетом уровней привилегий пользователей.
5. **Снижение административной нагрузки** за счет автоматизации рутинных операций (управление сессиями, мониторинг активности, восстановление паролей).
6. **Улучшение пользовательского опыта** благодаря удобному интерфейсу, быстрой аутентификации и упрощенным процедурам регистрации.
7. **Интеграцию с корпоративными системами** (CRM, ERP и др.) для обмена данными о пользователях и их правах доступа.

Реализация данной системы позволит повысить безопасность, эффективность и удобство работы с цифровыми ресурсами организации.

## Область и условия применения АС

**Автоматизированная система аутентификации и авторизации (АСАА)** предназначена для управления доступом пользователей к корпоративным информационным ресурсам, включая веб-приложения, внутренние сервисы и интегрированные системы.

## Ограничения применения АС

* **Автоматизированная система аутентификации и авторизации (АСАА)** имеет следующие ограничения в применении:
* **1. Технические ограничения**
* 1.1. **Серверная часть:**
* Работает только в средах, поддерживающих **.NET Core 3.1+/Java 11+/Node.js 16+** (в зависимости от реализации).
* Требует **выделенного сервера** с минимальными характеристиками:
* 4+ ядра CPU
* 8+ ГБ ОЗУ
* 100+ ГБ дискового пространства (SSD/NVMe)
* Поддерживает **только современные СУБД**: PostgreSQL 12+, Microsoft SQL Server 2019+, Oracle 19c+.
* 1.2. **Клиентская часть:**
* Совместима **только с актуальными версиями браузеров**:
* Google Chrome (последние 3 версии)
* Mozilla Firefox (последние 3 версии)
* Microsoft Edge (Chromium-based)
* Safari 14+ (только для macOS/iOS)
* Не поддерживает **Internet Explorer и устаревшие браузеры**.
* Для мобильных приложений требуется **Android 8.0+ / iOS 14+**.
* **2. Функциональные ограничения**
* 2.1. **Аутентификация:**
* Поддерживает **не более 3 методов MFA** (SMS, TOTP, E-mail, биометрия – на выбор).
* Не поддерживает **устаревшие протоколы** (NTLM, LDAP без TLS).
* 2.2. **Авторизация:**
* Максимальная глубина вложенности ролей – **5 уровней**.
* Не поддерживает **динамическое изменение прав во время активной сессии** (требуется повторная аутентификация).
* **3. Организационные ограничения**
* 3.1. **Администрирование:**
* Требует **назначенных администраторов** с соответствующими правами.
* Не предоставляет **полностью автономной работы** – необходим периодический мониторинг и обновления.
* 3.2. **Масштабируемость:**
* Без кластеризации поддерживает **до 10 000 активных пользователей**.
* Для больших нагрузок требуется **дополнительная настройка балансировщиков**.
* **4. Интеграционные ограничения**
* 4.1. **Совместимость:**
* Интеграция с внешними системами возможна **только через REST API/OAuth 2.0/SAML 2.0**.
* Не поддерживает **устаревшие форматы данных** (XML-RPC, SOAP 1.1).
* 4.2. **Кастомизация:**
* Изменение интерфейса аутентификации требует **доработки фронтенда**.
* Добавление новых методов MFA возможно **только через API.**

# ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС

## Требования к АС в целом

**Автоматизированная система аутентификации и авторизации (АСАА)** должна соответствовать следующим общим требованиям:

**1. Архитектура и технологическая платформа**

1.1. Система разрабатывается на основе **веб-технологий** по принципу **«сервер – тонкий клиент»**.  
1.2. Клиентский доступ обеспечивается **через стандартные интернет-браузеры** без необходимости установки дополнительного ПО.  
1.3. Серверная часть должна быть адаптирована для работы в **корпоративной ИТ-инфраструктуре** с учетом требований к безопасности и производительности.

**2. Доступ и взаимодействие**

2.1. **Пользовательский доступ:**

* Осуществляется через **веб-интерфейс** (HTML5, CSS3, JavaScript) с поддержкой адаптивного дизайна.
* Должна обеспечиваться **кросс-браузерная совместимость** (Chrome, Firefox, Edge, Safari).

2.2. **Интеграция с другими системами:**

* Взаимодействие с внешними ИС (CRM, ERP, Active Directory) должно поддерживаться через **REST API** или **GraphQL**.
* Для авторизации сторонних приложений должен использоваться **OAuth 2.0** или **SAML 2.0**.

**3. Безопасность и надежность**

3.1. **Защита данных:**

* Обязательное использование **HTTPS (TLS 1.2/1.3)** для всех соединений.
* Поддержка **многофакторной аутентификации (MFA)** (SMS, TOTP, биометрия).

3.2. **Устойчивость к атакам:**

* Реализация механизмов защиты от **Brute Force, SQL-инъекций, XSS, CSRF**.
* Автоматическая блокировка учетных записей при подозрительной активности.

**4. Производительность и масштабируемость**

4.1. **Серверные требования:**

* Минимальные характеристики сервера:
  + **4+ ядра CPU**
  + **8+ ГБ ОЗУ**
  + **100+ ГБ SSD/NVMe** (в зависимости от нагрузки).
* Поддержка **контейнеризации (Docker, Kubernetes)** для упрощения развертывания.

4.2. **Масштабируемость:**

* Возможность **горизонтального масштабирования** при увеличении числа пользователей.
* Поддержка **кеширования (Redis, Memcached)** для ускорения работы.

**5. Совместимость и адаптация**

5.1. **Адаптация под локальную инфраструктуру:**

* Интеграция с **корпоративными каталогами (Active Directory, LDAP)**.
* Поддержка **национальных стандартов шифрования и сертификации**.

5.2. **Клиентские требования:**

* Работа на **ПК, планшетах и смартфонах** с поддержкой **мобильных ОС (Android 8.0+, iOS 14+)**.
* Совместимость с **корпоративными VPN и прокси**.

## Требования к структуре и функционированию АС

## Модульная архитектура:

## Система должна состоять из независимых модулей:

## Модуль аутентификации

## Модуль авторизации

## Модуль аудита и мониторинга

## Модуль интеграции

## Функционирование:

## Круглосуточная работа (24/7/365)

## Максимальное время простоя - не более 15 минут в месяц

## Автоматическое восстановление после сбоев в течение 5 минут

## Масштабируемость:

## Поддержка увеличения нагрузки в 3 раза без изменения архитектуры

## Возможность добавления новых модулей без остановки работы

## Требования к защите информации от несанкционированного доступа

1. **Аутентификация**:
   * Многофакторная аутентификация (не менее 2 факторов)
   * Блокировка после 5 неудачных попыток входа
   * Минимальная сложность пароля: 12 символов (буквы, цифры, спецсимволы)
2. **Шифрование**:
   * TLS 1.2/1.3 для всех соединений
   * AES-256 для хранения конфиденциальных данных
   * Хэширование паролей с использованием PBKDF2 или bcrypt
3. **Контроль доступа**:
   * Ролевая модель (RBAC) с минимальными привилегиями
   * Разделение обязанностей (SoD)
   * Журналирование всех критических операций

## Требования по сохранности информации при авариях

1. **Резервное копирование**:
   * Ежедневные инкрементные копии
   * Полные копии раз в неделю
   * Хранение резервных копий в географически распределенном ЦОД
2. **Восстановление**:
   * Время восстановления (RTO) - не более 1 часа
   * Точка восстановления (RPO) - не более 15 минут
   * Автоматическое тестирование резервных копий раз в месяц

## Требования к информационному обеспечению

1. **Данные пользователей**:
   * Хранение только необходимых данных
   * Соблюдение GDPR и других регуляторных требований
   * Возможность экспорта/импорта данных в стандартных форматах
2. **Метаданные**:
   * Ведение журнала изменений конфигурации
   * Хранение истории действий пользователей (не менее 3 лет)

## Требования к математическому обеспечению

1. **Алгоритмы**:
   * Криптографические алгоритмы, сертифицированные ФСТЭК/ФСБ
   * Оптимизированные алгоритмы поиска и сортировки
   * Алгоритмы машинного обучения для выявления аномалий
2. **Расчеты**:
   * Точность вычислений - не менее 99.99%
   * Поддержка высокоточных временных меток

## Требования к программному обеспечению

1. **Серверная часть**:
   * Поддержка Java 11+/.NET Core 3.1+/Node.js 16+
   * Контейнеризация (Docker)
   * Оркестрация (Kubernetes)
2. **Клиентская часть**:
   * Поддержка современных браузеров (Chrome, Firefox, Edge, Safari)
   * Progressive Web App (PWA) для мобильных устройств

## Требования к организационному обеспечению

1. **Персонал**:
   * Минимум 2 администратора с разными правами
   * Обязательное обучение и сертификация
2. **Процедуры**:
   * Регламент изменения прав доступа
   * Политика реагирования на инциденты
   * План аварийного восстановления

## Требования к патентной чистоте

1. **Лицензии**:
   * Использование только лицензионного ПО
   * Открытое ПО только с разрешения юридического отдела
   * Проверка на соответствие экспортному контролю

## Требования к документированию

1. **Техническая документация**:
   * Полное описание API
   * Руководство администратора
   * Руководство пользователя
   * Документация по интеграции
2. **Форматы**:
   * PDF для конечных пользователей
   * Markdown/AsciiDoc для разработчиков
   * Swagger/OpenAPI для API

## Требования к функциям (задачам), выполняемым подсистемами

1. **Подсистема аутентификации**:
   * Поддержка различных методов аутентификации
   * Защита от брутфорса
   * Управление сессиями
2. **Подсистема авторизации**:
   * Динамическое управление правами
   * Проверка прав в реальном времени
   * Делегирование полномочий
3. **Подсистема аудита**:
   * Журналирование всех критических событий
   * Генерация отчетов
   * Уведомления о подозрительной активности
4. **Подсистема интеграции**:
   * Поддержка стандартных протоколов (OAuth 2.0, SAML)
   * API для внутренней интеграции
   * Webhooks для внешних систем

# 

# 6.СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА

**Общий срок реализации проекта** составляет **9 месяцев** от даты подписания договора до полного ввода системы в промышленную эксплуатацию.

**Основные этапы и сроки выполнения:**

1. **Подготовительный этап (1 месяц)**
   * Формирование и согласование технического задания
   * Анализ существующей инфраструктуры
   * Определение требований к интеграции
2. **Проектирование (1,5 месяца)**
   * Разработка архитектуры системы
   * Создание технического проекта
   * Проектирование баз данных и API
   * Разработка схем безопасности
3. **Разработка основных модулей (3 месяца)**
   * Реализация ядра аутентификации
   * Разработка механизма авторизации
   * Создание панели администратора
   * Разработка интерфейсов пользователя
4. **Интеграционные работы (1 месяц)**
   * Подключение к корпоративным системам
   * Настройка API-шлюзов
   * Тестирование интеграционных решений
5. **Комплексное тестирование (1,5 месяца)**
   * Функциональное тестирование
   * Нагрузочное тестирование
   * Тестирование безопасности (пентест)
   * Исправление выявленных недостатков
6. **Пилотная эксплуатация (1 месяц)**
   * Развертывание тестового контура
   * Обучение администраторов
   * Сбор обратной связи
   * Доработка системы
7. **Промышленная эксплуатация (1 месяц)**
   * Развертывание продуктивного контура
   * Перенос данных
   * Окончательная настройка
   * Подписание акта ввода в эксплуатацию

**Ключевые контрольные точки проекта:**

* Через 4 месяца - завершение разработки MVP с базовой функциональностью
* Через 7 месяцев - готовность полной версии системы
* Через 9 месяцев - полное завершение проекта

**Условия изменения сроков:**  
Сроки могут быть пересмотрены в случае:

* Существенного изменения требований (не более чем на 15% от исходных сроков)
* Возникновения форс-мажорных обстоятельств
* Задержек согласований со стороны заказчика

**Гарантийные обязательства:**  
После ввода системы в эксплуатацию предусматривается:

* 3 месяца гарантийного сопровождения
* 12 месяцев постгарантийной поддержки (по отдельному соглашению)

**Примечание:** Представленные сроки являются предварительными и могут быть уточнены при заключении договора на основании детального обследования инфраструктуры заказчика и окончательного технического задания.

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