Управление торговой системы авторизации и управления доступом

(наименование объекта автоматизации)

3

(класс автоматизированной системы)

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ**

**К РАЗРАБОТКЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АВТОРИЗАЦИИ И УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ ТОРГОВЫХ УСЛУГ**

**(АС АУДТУ)**

На 12 листах

**ОГЛАВЛЕНИЕ**

[**1** **ОБЩИЕ СВЕДЕНИЯ** 3](#_Toc194536470)

[**2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ** 3](#_Toc194536471)

[**3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ** 5](#_Toc194536472)

[**4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС** 7](#_Toc194536473)

[**5 ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС** 9](#_Toc194536474)

[**6 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА** 11](#_Toc194536475)

1. **ОБЩИЕ СВЕДЕНИЯ**

1.1 Наименование работы:  
Разработка технических требований к автоматизированной системе авторизации и управления доступом для предприятий торгового сектора (АС АУДТУ).

* 1. Заказчик и исполнитель:
  + Заказчик: Министерство торговли Республики Беларусь
  + Исполнитель: Департамент цифровых технологий Министерства торговли

1.3 Организации-пользователи:

* + Розничные торговые сети
  + Оптовые поставщики товаров
  + Маркетплейсы и электронные торговые площадки
  + Логистические компании, интегрированные с торговыми платформами

1.4 Объект автоматизации:  
Единая платформа управления доступом к торговым операциям, включая:

* + Системы онлайн-заказов
  + Управление складскими запасами
  + Персонализированные сервисы для клиентов
  + Аналитические инструменты для бизнеса

**2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ**

2.1 В настоящих технических требованиях применены термины и определения в следующем значении:

2.1.1 Автоматизированная торговая система (АТС) - комплекс программно-аппаратных средств, предназначенный для автоматизации процессов авторизации, управления доступом и обработки транзакций в сфере розничной и оптовой торговли.

2.1.2 Торговая авторизация - процесс проверки и подтверждения прав пользователя на совершение определенных операций в торговой системе, таких как оформление заказов, доступ к складским остаткам или управление ценами.

2.1.3 Многоуровневая аутентификация - процедура подтверждения личности пользователя, включающая как минимум два из следующих факторов:

* Знание (логин/пароль)
* Владение (мобильное устройство для SMS-кода)
* Свойство (биометрические данные)

2.1.4 Торговый оператор - уполномоченный сотрудник торговой организации, имеющий расширенные права доступа к функционалу системы, включая управление товарным каталогом, обработку возвратов и формирование отчетности.

2.1.5 Сессия доступа - временной промежуток, в течение которого пользователь может работать с системой без повторной авторизации, ограниченный по времени и функциональным возможностям.

2.1.6 Динамический контроль доступа - механизм автоматической корректировки прав пользователя в зависимости от:

* Текущего статуса клиента
* Проводимых маркетинговых акций
* Географического местоположения
* Времени суток

2.2 В настоящих технических требованиях использованы следующие сокращения:

|  |  |  |
| --- | --- | --- |
| **Сокращение** | **Полное наименование** | **Описание** |
| АТС | Автоматизированная торговая система | Основная платформа системы |
| СУПД | Система управления правами доступа | Подсистема распределения прав |
| ТПК | Торговый профиль клиента | Учетная запись пользователя |
| API-Шлюз | Программный интерфейс интеграции | Обеспечивает связь с внешними системами |
| PCI DSS | Payment Card Industry Data Security Standard | Стандарт безопасности платежных данных |

2.3 Дополнительные определения:

2.3.1 Привилегированный доступ - особые права, предоставляемые администраторам системы для:

* Управления учетными записями пользователей
* Настройки параметров безопасности
* Обработки критических инцидентов

2.3.2 Аварийный доступ - специальный режим авторизации, активируемый при:

* Сбоях в основном канале аутентификации
* Необходимости экстренного вмешательства
* Проведении технических работ

2.3.3 Сессионный токен - уникальный цифровой идентификатор, генерируемый системой для:

* Отслеживания активности пользователя
* Защиты от несанкционированного доступа
* Обеспечения непрерывности работы при переключении между устройствами

2.4 Классификация пользователей:

2.4.1 Категории пользователей:

* Покупатели (физические лица)
* Торговые представители (сотрудники магазинов)
* Менеджеры товарных групп
* Администраторы сети
* Системные интеграторы

2.4.2 Уровни доступа:

* Базовый (просмотр каталога)
* Операционный (оформление заказов)
* Административный (управление системой)
* Аудиторский (просмотр логов и отчетов)

**3 ХАРАКТЕРИСТИКА ОБЪЕКТА ВНЕДРЕНИЯ**

3.1 Перечень и краткая характеристика бизнес-процессов

3.1.1 Объектом автоматизации является система авторизации и управления доступом для предприятий торгового сектора, обеспечивающая:

* Безопасный вход пользователей в торговые платформы
* Контроль прав доступа к функционалу системы
* Защиту персональных и финансовых данных

3.1.2 Процесс авторизации осуществляется на трех уровнях:

* Клиентский уровень:
  + Регистрация новых пользователей
  + Восстановление доступа
  + Управление личным кабинетом
* Операционный уровень:
  + Аутентификация сотрудников
  + Управление ролевой моделью
  + Контроль сессий
* Административный уровень:
  + Настройка политик безопасности
  + Мониторинг подозрительной активности
  + Управление криптографическими ключами

3.1.3 Основные технологические процессы включают:

* Верификацию пользователей при входе
* Проверку прав доступа при выполнении операций
* Автоматическое завершение неактивных сессий
* Ведение журнала событий безопасности

3.2 Требования к входным и выходным данным

3.2.1 Входные данные:

* Учетные данные пользователей (логины, пароли, биометрические данные)
* Токены сессий
* Параметры доступа (роли, привилегии)
* Данные об устройствах доступа

3.2.2 Выходные данные:

* Результаты аутентификации (успешная/неуспешная)
* Текущие права доступа
* Статистика использования системы
* Предупреждения о подозрительной активности

3.2.3 Форматы представления данных:

Таблица 3.1 - Форматы данных авторизации

|  |  |  |
| --- | --- | --- |
| **Параметр** | **Формат** | **Пример** |
| Идентификатор пользователя | Числовой (12 знаков) | 123456789012 |
| Результат аутентификации | Булево значение | true/false |
| Уровень доступа | Строка (20 символов) | "manager", "admin" |
| Время сессии | Дата-время (ISO 8601) | 2024-02-20T14:30:00+03:00 |

3.3 Выполняемые технологические операции

3.3.1 Основные операции системы:

* Операции аутентификации:
  + Проверка учетных данных
  + Генерация сессионных токенов
  + Валидация биометрических данных
* Операции авторизации:
  + Проверка прав доступа
  + Применение политик безопасности
  + Обработка исключительных ситуаций
* Административные операции:
  + Управление пользователями
  + Настройка ролевой модели
  + Анализ журналов безопасности

3.3.2 Технологический процесс включает:

* Прием запроса на авторизацию
* Валидацию входных параметров
* Проверку соответствия политикам безопасности
* Формирование ответа
* Логирование операции

3.3.3 Требования к производительности:

* Время обработки запроса авторизации - не более 500 мс
* Поддержка не менее 1000 одновременных сессий
* Обработка до 50 авторизаций в секунду

**4 ЦЕЛИ И УСЛОВИЯ СОЗДАНИЯ АС**

4.1 Формулировка цели разработки

4.1.1 Основной целью создания АС АУДТУ является:

* Построение единой защищенной платформы управления доступом для участников торгового сектора
* Автоматизация процессов идентификации и аутентификации пользователей
* Обеспечение безопасного взаимодействия между различными компонентами торговой инфраструктуры

4.1.2 Ключевые технологические цели:

* Сокращение времени обработки запросов авторизации на 40% по сравнению с существующими решениями
* Достижение 99,9% доступности системы
* Обеспечение соответствия международным стандартам безопасности (PCI DSS, ISO 27001)

4.2 Область и условия применения

4.2.1 Система предназначена для использования:

* В розничных торговых сетях
* На электронных торговых площадках
* В системах управления складскими комплексами
* В платежных и логистических сервисах

4.2.2 Условия эксплуатации:

* Круглосуточный режим работы
* Поддержка территориально распределенной инфраструктуры
* Интеграция с существующими ERP и CRM системами

4.2.3 Основные пользовательские сценарии:

* Массовая авторизация покупателей в часы пик
* Управление доступом поставщиков к товарным каталогам
* Контроль действий кассиров и менеджеров

4.3 Ограничения применения

4.3.1 Технические ограничения:

* Совместимость только с ОС Windows Server 2019+ и Linux (CentOS 7+)
* Требование к каналу связи - не менее 10 Мбит/с на точку доступа
* Не поддерживаются мобильные устройства с ОС старше Android 8/iOS 12

4.3.2 Функциональные ограничения:

* Отсутствие встроенной поддержки блокчейн-аутентификации в базовой версии
* Ограничение на длину пароля (не более 64 символов)
* Максимальное количество ролей в системе - 256

4.3.3 Организационные ограничения:

* Необходимость наличия выделенного администратора безопасности
* Обязательное обучение персонала перед вводом в эксплуатацию
* Требование к резервному копированию данных не реже 1 раза в сутки

4.3.4 Правовые ограничения:

* Соответствие законодательству о защите персональных данных
* Необходимость сертификации в регулирующих органах
* Ограничения на использование криптографических алгоритмов

4.4 Экономические показатели

4.4.1 Ожидаемый экономический эффект:

* Снижение затрат на администрирование доступа на 25-30%
* Уменьшение потерь от мошенничества на 15-20%
* Сокращение времени обработки инцидентов безопасности в 2 раза

4.4.2 Нормативные показатели:

* Срок окупаемости - не более 2 лет
* Годовые затраты на поддержку - не более 5% от стоимости внедрения
* Плановый срок эксплуатации - 5 лет

**5 ФУНКЦИИ И ЗАДАЧИ СОЗДАВАЕМОЙ АС**

5.1 Требования к системе в целом

5.1.1 Архитектурные требования

* Клиент-серверная архитектура с веб-интерфейсом
* Поддержка горизонтального масштабирования
* Резервирование критических компонентов

5.1.2 Требования к безопасности

* Многофакторная аутентификация (SMS, TOTP, биометрия)
* Шифрование данных при передаче (TLS 1.2+)
* Хранение паролей с использованием адаптивного хеширования (Argon2id)
* Защита от brute-force атак

5.1.3 Требования к надежности

* Время безотказной работы ≥ 99.95%
* Автоматическое восстановление после сбоев
* Резервное копирование данных каждые 4 часа

5.2 Требования к подсистемам

5.2.1 Подсистема аутентификации

* Регистрация новых пользователей
* Восстановление доступа
* Управление учетными данными
* Интеграция с Active Directory/LDAP

5.2.2 Подсистема авторизации

* Ролевая модель доступа (RBAC)
* Контекстно-зависимые политики
* Временные ограничения доступа
* Делегирование полномочий

5.2.3 Подсистема аудита

* Журналирование всех событий безопасности
* Генерация отчетов
* Оповещения о подозрительной активности
* Интеграция с SIEM-системами

5.3 Требования к интерфейсам

5.3.1 Пользовательские интерфейсы

* Адаптивный веб-интерфейс
* Мобильное приложение (iOS/Android)
* API для интеграции

5.3.2 Программные интерфейсы

* REST API с OAuth 2.0 авторизацией
* Webhooks для событий безопасности
* Поддержка SAML 2.0/OIDC

5.4 Требования к производительности

* Время отклика ≤ 500 мс для 95% запросов
* Поддержка ≥ 1000 одновременных сессий
* Обработка ≥ 50 транзакций/сек

5.5 Требования к данным

5.5.1 Форматы данных

* JSON для API
* XML для интеграции с ERP
* CSV для отчетов

5.5.2 Хранение данных

* Шифрование данных на rest
* Хранение журналов ≥ 1 года
* Гео-репликация критических данных

5.6 Требования к совместимости

* Поддержка современных браузеров (Chrome, Firefox, Safari, Edge)
* Совместимость с Windows/Linux серверами
* Интеграция с популярными CRM/ERP системами

5.7 Специальные требования

5.7.1 Для торговых сетей

* Поддержка POS-терминалов
* Интеграция с кассовыми системами
* Оффлайн-авторизация

5.7.2 Для электронной коммерции

* Защита от кардинга
* Интеграция с платежными системами
* Защита API от злоупотреблений

5.8 Требования к сопровождению

* Централизованное управление конфигурацией
* Механизм автоматических обновлений
* Удаленный мониторинг состояния системы
* Поддержка нескольких версий API

**6 СРОКИ ВЫПОЛНЕНИЯ ПРОЕКТА**

6.1 Основные этапы разработки

1. Подготовка ТЗ - 1 месяц
2. Проектирование архитектуры - 2 месяца
3. Разработка ядра системы - 3 месяца
4. Тестирование - 1 месяц
5. Ввод в эксплуатацию - 1 месяц

6.2 График выполнения работ

|  |  |  |
| --- | --- | --- |
| **Этап** | **Срок выполнения** | **Ответственные** |
| Анализ требований | 01.03-15.03 | Аналитики |
| Разработка прототипа | 16.03-30.04 | Разработчики |
| Тестирование | 01.05-31.05 | QA-инженеры |
| Внедрение | 01.06-30.06 | Внедренцы |

6.3 Условия приемки

* Соответствие 100% требований ТЗ
* Успешное прохождение нагрузочных тестов
* Подписание акта сдачи-приемки

6.4 Гарантийные обязательства

* Гарантийный срок - 12 месяцев
* Критические исправления - в течение 24 часов
* Обновления безопасности - ежеквартально

6.5 Требования к инфраструктуре

* Сервер: 4 ядра, 16ГБ RAM, 200ГБ HDD
* ОС: Windows Server 2016+/Linux CentOS 7+
* СУБД: PostgreSQL 12+/MySQL 8+

6.6 Обучение персонала

* Базовый курс - 8 часов
* Администрирование - 16 часов
* Предоставление инструкций и мануалов

**НАСТОЯЩИЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ МОГУТ БЫТЬ УТОЧНЕНЫ И КОРРЕКТИРОВАНЫ ПО ВЗАИМНОЙ ДОГОВОРЕННОСТИ МЕЖДУ ЗАКАЗЧИКОМ И ИСПОЛНИТЕЛЕМ В РАБОЧЕМ ПОРЯДКЕ.**