

ООО «Иксими»

**Описание функциональных характеристик
программного обеспечения
«Интеллектуальная корпоративная система
интеграционного менеджмента информации
"ИКСИМИ:АГЕНТ 6.4"»**

г. Зеленодольск

2026 год

Настоящий документ содержит описание функциональных характеристик программного обеспечения «Интеллектуальная корпоративная система интеграционного менеджмента информации "ИКСИМИ:АГЕНТ 6.4"»

Назначение и область применения

Программное обеспечение «Интеллектуальная корпоративная система интеграционного менеджмента информации "ИКСИМИ:АГЕНТ 6.4"» предназначено и применяется для Автоматизация обработки корпоративных данных и бизнес-процессов предприятия на основе технологий искусственного интеллекта и больших языковых моделей

Функциональные задачи

ПО обеспечивает решение следующих задач:

1. Приём и обработка запросов пользователей

Задача: Обеспечение единой точки входа для всех запросов пользователей на естественном языке через стандартизированный API и интерфейс MAX.

Описание: ПО принимает входящие запросы от пользователей через REST API (эндпоинты /process, /approval, /diff, /merge) и через MAX-бота. Осуществляется аутентификация пользователей по API-токену или MAX ID, авторизация доступа к проектам, валидация входных параметров. Каждый запрос получает изолированную сессию с собственным рабочим пространством.

2. Оркестрация вызовов инструментов (Tool Calling)

Задача: Автоматический выбор и последовательный вызов инструментов для выполнения задач пользователя.

Описание: ПО реализует итеративный цикл взаимодействия с LLM: система передаёт модели список доступных инструментов (schemas), LLM возвращает вызов инструмента, система выполняет его и передаёт результат обратно в LLM. Цикл продолжается до получения финального ответа или достижения лимита итераций (по умолчанию 10). Поддерживаются параллельные вызовы, обработка ошибок и автоматическая адаптация к результатам.

3. Интеграция с учётными системами (1С:Предприятие, Битрикс 24)

Задача: Обеспечение доступа к корпоративным данным и автоматизации операций в учётных системах.

Описание: ПО взаимодействует с 1С:Предприятие и Битрикс 24 через стандартные открытые интерфейсы (OData, HTTP-сервисы). Интеграция реализована через абстракцию внешнего провайдера: продукт не содержит кода 1С/Битрикс 24 и не требует её модификации. Поддерживается чтение данных (контрагенты, организации, номенклатура, счета) и создание документов (счета на оплату) с обязательным подтверждением пользователя для операций записи.

4. Маршрутизация к специализированным экспертам (Mixture of Experts)

Задача: Повышение качества ответов путём выбора наиболее подходящей

языковой модели для каждой предметной области.

Описание: ПО реализует инструмент `domain_expert`, который маршрутизирует запросы к специализированным языковым моделям в зависимости от области знаний: металлургия, юриспруденция, медицина, финансы, инженерия, IT. Каждая предметная область имеет собственную системную инструкцию и параметры генерации (температура, ограничение токенов).

5. Автоматическое изменение исходного кода проектов

Задача: Внесение изменений в код проектов по запросу пользователя на естественном языке.

Описание: ПО реализует инструмент `code_edit` с поддержкой трёх операций: полная запись файла (`write`), удаление (`delete`) и применение унифицированного diff-патча (`patch`) с валидацией контекста и синтаксиса. Изменения вносятся только в изолированную рабочую копию проекта, оригинал не модифицируется до подтверждения пользователя. Поддерживается автоматическое создание бэкапа и механизм отката.

6. Управление подтверждениями опасных операций (Approval Flow)

Задача: Обеспечение контроля пользователя над потенциально опасными действиями системы.

Описание: ПО реализует механизм подтверждения для операций, изменяющих данные: изменение кода, выполнение `shell`-команд, обработка медиафайлов, создание документов в 1С, Битрикс 24. При необходимости подтверждения система приостанавливает выполнение цикла, сохраняет полное состояние сессии и запрашивает согласие пользователя. После подтверждения или отклонения выполнение возобновляется с сохранённого места.

7. Изоляция сессий пользователей

Задача: Обеспечение безопасности при одновременной работе нескольких пользователей.

Описание: Каждый запрос пользователя выполняется в изолированной сессии с собственным рабочим пространством. ПО гарантирует, что инструменты не имеют доступа к данным других сессий, а рабочая копия проекта создаётся индивидуально для каждой сессии. Реализована потокобезопасная архитектура инструментов (`stateless tools`).

8. Получение данных из сети интернет

Задача: Обеспечение работы с внешними источниками данных.

Описание: ПО реализует инструмент `web_fetch` для получения данных по указанному URL через HTTP-клиент и парсинга HTML. Для поиска информации в сети реализован опциональный модуль `web_search` с поддержкой поисковых провайдеров (Yandex Search API). Модуль поиска подключается через конфигурацию и может быть отключен без потери основной функциональности.

9. Аудит и протоколирование действий

Задача: Ведение полного журнала действий системы для контроля и разбора инцидентов.

Описание: ПО логирует все вызовы инструментов, результаты их выполнения, решения о подтверждении, изменения файлов. Ведётся статистика по сессиям,

запросам, вызовам инструментов, ошибкам аутентификации. Данные сохраняются в структурированном виде и доступны для анализа.

Функциональные возможности

1. Автоматизация обработки корпоративных данных на естественном языке
Приём запросов пользователей и выполнение операций в учётных системах.
2. Интеллектуальный поиск и анализ данных
Поиск информации в корпоративных базах данных и внешних источниках.
3. Автоматическое создание документов
Создание счетов на оплату, работа с номенклатурой и контрагентами.
4. Экспертные консультации по предметным областям
Маршрутизация к специализированным языковым моделям.
5. Автоматическое изменение кода проектов
Внесение изменений в исходный код с подтверждением и откатом.
6. Диалоговое взаимодействие через MAX
Работа через MAX-бота с выбором проектов и подтверждением действий.
7. Модульная расширяемость
Подключение новых инструментов и поисковых провайдеров через конфигурацию.
8. Полная автономность
Работа без обязательной зависимости от внешних сервисов.

Входные данные

Запрос пользователя на естественном языке

- Источник: REST API / MAX-бот
- Формат: JSON
- Описание: Текст запроса на естественном языке, идентификатор целевого проекта, учётные данные пользователя

Данные для аутентификации

- Источник: HTTP-заголовки / MAX
- Формат: Bearer-токен / MAX ID
- Описание: Удостоверение пользователя для проверки прав доступа к системе и проектам

Данные из учётной системы 1С

- Источник: 1С:Предприятие
- Формат: JSON (OData, HTTP-сервисы)
- Описание: Контрагенты, организации, номенклатура, счета на оплату, реквизиты

Данные из сети интернет

- Источник: Веб-ресурсы
- Формат: HTML, текст
- Описание: Получение данных по указанному URL через web_fetch; опционально — поиск через сменные провайдеры

Подтверждения опасных операций

- Источник: Пользователь
- Формат: JSON (session_id, approval_id, approved)

- Описание: Согласие или отказ на выполнение операций, требующих approval (code_edit, run_cli, 1c_create_invoice, bitrix_create_invoice)

Выходные данные

Финальный ответ пользователю

- Получатель: REST API / MAX-бот
- Формат: JSON / текст
- Описание: Обработанный ответ агента на запрос пользователя, включая текстовую часть и структурированные данные

Список вызовов инструментов

- Получатель: Пользователь / API
- Формат: JSON
- Описание: Полная история tool calls с параметрами, результатами и статусом выполнения

Diff изменений проекта

- Получатель: Пользователь
- Формат: Unified diff / JSON
- Описание: Изменения в файлах (added, modified, deleted) с информацией о бэкапе

Запрос на подтверждение

- Получатель: Пользователь
- Формат: JSON (approval_id, description, session_id)
- Описание: Запрос approval для опасных операций, отображаемый через inline-кнопки в MAX или через API

Данные из 1C

- Получатель: Пользователь / LLM
- Формат: JSON
- Описание: Список контрагентов, организаций, номенклатуры, счетов, реквизитов

Статистика системы

- Получатель: Администратор / API
- Формат: JSON
- Описание: Метрики по сессиям, запросам, вызовам инструментов, ошибкам аутентификации

Архитектура ПО

Архитектура приложения реализована следующим образом:

1. Пользователь отправляет запрос на естественном языке через REST API или MAX-бота.
2. Система выполняет аутентификацию пользователя и проверку прав доступа.
3. Создаётся изолированная сессия с собственным рабочим пространством, при необходимости — рабочая копия проекта.
4. Оркестратор передаёт запрос и список доступных инструментов в языковую модель (LLM).
5. LLM возвращает вызов инструмента, система выполняет его и передаёт результат обратно.

6. Цикл повторяется до получения финального ответа. Для опасных операций — запрос подтверждения пользователя.
7. Изменения вносятся в рабочую копию, оригинал обновляется только по команде /merge с созданием бэкапа.

Взаимодействие между компонентами

Этапы взаимодействия

1. Пользователь → Система (REST API / MAX)

Пользователь отправляет запрос на естественном языке.

Система аутентифицирует пользователя и проверяет права доступа к проекту.

2. Система → LLM (Tool Calling)

Оркестратор формирует сообщения: системная инструкция, история диалога, запрос пользователя.

Передаёт список доступных инструментов (JSON Schema).

LLM возвращает ответ с вызовом инструмента или финальный текст.

3. Система → Инструменты (выполнение)

Для каждого вызова система проверяет политику безопасности (Policy).

Если требуется подтверждение — сохраняет состояние и запрашивает approval.

Выполняет инструмент в изолированном workspace сессии.

4. Система → Учётная система 1С (интеграция)

Через стандартные интерфейсы (OData, HTTP-сервисы) выполняется чтение или запись данных.

Операции записи требуют подтверждения пользователя.

5. Система → Внешние источники (web)

Через web_fetch загружаются данные по указанному URL.

Опциональный web_search маршрутизирует запрос к выбранному поисковому провайдеру.

6. Система → Пользователь (ответ)

Финальный ответ передаётся пользователю.

При наличии изменений — пользователь может просмотреть diff (/diff) и применить его (/merge).

7. Администрирование

Администратор управляет пользователями, правами доступа, проектами через API и конфигурацию.

Требования к техническим средствам (Эксплуатационные характеристики)

Для установки и эксплуатации программного обеспечения «Интеллектуальная корпоративная система интеграционного менеджмента информации "ИКСИМИ:АГЕНТ 6.4"» необходимо, чтобы аппаратное обеспечение соответствовало следующим требованиям:

ЦП: x86_64 архитектура, от 4 ядер.

ОЗУ: от 8 ГБ (зависит от размера используемой языковой модели).

Дисковая подсистема: SSD от 50 ГБ (зависит от размера загруженной языковой модели и проектов).

GPU (опционально): от 8 ГБ VRAM для ускорения инференса LLM.

ОС: Рекомендуется Astra Linux, ОСнова.

Поддержка:

- Дистрибутив Linux с поддержкой Python 3.10+ (Debian, Ubuntu),

- Windows 10/11 с WSL2.

Дополнительно: Python 3.10+, Ollama или совместимый LLM-сервер, 1С:Предприятие 8.3+, Битрикс 24 (опционально, лицензия пользователя).

Описание функциональной части программного обеспечения

Языки программирования программного обеспечения «Интеллектуальная корпоративная система интеграционного менеджмента информации "ИКСИМИ:АГЕНТ 6.4" », –Python и JavaScript

Информация, необходимая для установки и эксплуатации

Для установки и правильной эксплуатации «Интеллектуальная корпоративная система интеграционного менеджмента информации "ИКСИМИ:АГЕНТ 6.4"» необходимо ознакомиться с информацией, размещенной в Руководстве пользователя.