Описание функциональных характеристик программного обеспечения «CapyAgent»

Редакция: CapyAgent Beta | Версия: 0.21.1 (ревизия ca5813fb) | Правообладатель: ИП Смольников Кирилл Георгиевич

1. Общие сведения и назначение

Программное обеспечение «CapyAgent» представляет собой прикладную программную платформу интеллектуального агента и оркестратора задач для персональных компьютеров и серверов. Программа принимает задания от пользователя на естественном русском языке, строит план действий, обращается к выбранной языковой модели, безопасно вызывает инструменты операционной системы, браузера и корпоративных сервисов, сохраняет долговременную память и возвращает готовый результат.

CapyAgent разработан как прикладное ПО оркестрации и не привязан к одной языковой модели. Программа включает единую точку подключения моделей и поддерживает отечественный облачный сервис подписки Capy AI (тарифные модели Capy Pro и Capy Flash), российские платформы YandexGPT и GigaChat (включая проверку TLS по корневому сертификату НУЦ Минцифры России), а также полностью автономные локальные модели на базе Ollama, vLLM и совместимых серверов OpenAI-формата.

Программа распространяется правообладателем (ИП Смольников Кирилл Георгиевич) на условиях лицензии Business Source License 1.1 (BSL 1.1, полный текст размещен по адресу https://capyagent.ru/ru/docs/reestr/LICENSE-BSL-1.1.txt): использование для собственных задач и внутри организации бесплатно, коммерческое внедрение клиентам и SaaS требуют лицензии правообладателя.

2. Архитектура и состав функциональных модулей

Программный комплекс объединяет серверную часть на Python 3.11-3.13, локальный веб-интерфейс на TypeScript/React, настольную оболочку Electron и кроссплатформенный установщик на Rust/Tauri. Для локального хранения сессий, долговременной памяти и индексов используется встроенная СУБД SQLite 3 с полнотекстовым поиском FTS5.

Модуль	Функциональное назначение
M01. Ядро агентного цикла (agent/)	Управление пошаговым циклом диалога, сжатие длинного контекста, защита от зацикливания повторов текста и инструментов (repetition_guard, tool_guardrails), автоматическое восстановление при сбоях, долговременная память с куратором и поиском FTS5.
M02. CLI, TUI и локальный API-сервер (capyagent_cli/, ui-tui/, tui_gateway/)	Консольный запуск (команды capy и capyagent), интерактивный терминальный интерфейс, локальный HTTP/WebSocket-сервер на базе FastAPI/Uvicorn, мастер первичной настройки, диагностика (capyagent doctor) и экспорт сессий.
M03. Веб-панель и UI-библиотека (web/, packages/capyagent-ui/)	Локальная веб-панель управления чатами, профилями, моделями, квотой, навыками и расписаниями. Включает собственную библиотеку компонентов @capyagent/ui и интерактивный визуальный индикатор состояния CapyMascot.
M04. Настольное приложение и установщик (apps/)	Десктоп-клиент на базе Electron с поддержкой локального и удаленного подключения к агенту, а также установщик среды на Rust/Tauri с раздельным хранением профилей.
M05. Многоканальный шлюз сообщений (gateway/)	Прием и отправка сообщений через Telegram (включая топики и голосовые сообщения), ВКонтакте, мессенджер MAX, электронную почту и другие платформы с защитой от циклических ответов бот-бот (BotLoopGuard).

Модуль	Функциональное назначение
M06. Инструменты, браузер и защита (tools/, acp_adapter/, native/)	Безопасное выполнение команд оболочки, чтение и извлечение таблиц и документов (XLSX, DOCX, PDF), управление браузером (включая видимую пользовательскую сессию с передачей управления для ввода паролей и 2FA), нативное управление окнами ОС через @ref-метки (agent-desktop), проверка навыков SkillsGuard.
M07. Подсистема провайдеров моделей (providers/, plugins/)	Единый реестр поставщиков моделей: отечественный провайдер Capy AI (авторизация кодом устройства через lk.capyagent.ru), YandexGPT, GigaChat, локальные серверы моделей и маршрутизация с резервным переключением (fallback).
M08. Российские MCP-коннекторы (connectors/)	Комплект из 11 встроенных MCP-серверов к российским бизнес-сервисам по протоколу stdio (подробный состав приведен в разделе 4).
M09. Планировщик задач (cron/)	Выполнение периодических поручений и напоминаний по расписанию cron с доставкой отчетов в выбранный мессенджер или файл.
M10. Навыки и локализация (skills/, optional-skills/, locales/)	Библиотека из 74 базовых и 156 опциональных процедурных навыков (из них 19 подгружаются по требованию пользователя), 17 языковых словарей с полным переводом на русский язык (locales/ru.yaml).

3. Управление безопасностью и правами доступа

CapyAgent разграничивает уровень самостоятельности агента через политику подтверждений approvals.mode и защитные фильтры:

- Режим «Всегда спрашивать» (manual) - любая потенциально опасная команда оболочки, запись или внешнее действие останавливается до явного подтверждения человеком в интерфейсе или мессенджере.
- Режим «Авто» (smart) - команда проверяется моделью-контролером с ограничителем последовательных отказов (circuit breaker).
- Режим «Полный доступ» (off) - автономное выполнение в изолированной среде или выделенной песочнице.
- Механизм SkillsGuard проверяет подключаемые навыки по шкале риска (0-100), блокирует скрытые управляющие символы Unicode, инъекции и несанкционированную передачу данных.
- Все секреты и токены хранятся в локальном файле .env и исключаются из журналов работы и контекста языковой модели.

4. Интеграция с российскими сервисами

Коннектор	Назначение	Режим доступа и защита
bitrix24	CRM Битрикс24: разведка структуры, поля сущностей, выгрузка сделок, лидов, компаний и контактов	Строго только чтение (белый список методов API)
yandex_direct	Яндекс Директ: статистика кампаний, отчеты и лимиты баллов API	Строго только чтение (методная блокировка записи)
mail / yandex_mail	Почта Яндекс, Mail.ru / ВК Почта и custom IMAP/SMTP: поиск писем, вложения, переписка	Отправка и перемещение выключены по умолчанию
yandex_search	Поиск по российскому сегменту сети через Search API Яндекс Облака	Только чтение
uis	Телефония UIS: история звонков, пропущенные вызовы, заявки с форм	Только чтение

Коннектор	Назначение	Режим доступа и защита
roistat	Сквозная аналитика Roistat: проекты, показатели и разведка схемы	Только чтение
vk	Сообщения сообществ ВКонтакте: диалоги и обработка обращений	Отправка сообщений требует отдельного включения
max	Мессенджер MAX: чтение чатов, поиск, вложения, расшифровка голосовых	Только чтение по умолчанию
telegram_user	Работа с Telegram-чатами от лица пользователя через Telethon	Белый список разрешенных чатов на запись
meetscribe + telemost-calls	Запись и расшифровка звонков Яндекс Телемоста и других платформ, подготовка протокола в DOCX	Локальная запись протокола в рабочий каталог
zenmoney	Управленческий и финансовый учет Дзен-мани: счета и операции	Запись только после явного подтверждения