

Подробный паспорт Штурвала

Тимон Ядро · Архитектор и разработчик интеграции

Редакция 2026-09-15 · Редакция 15 сентября 2026 года; состояние функций уточняется документом готовности

Область применимости и актуальные ограничения:
<https://team-on.ru/yadro/docs/readiness.html>

Оглавление

Область применения источника

1. Цель и смысл
 2. Пользователи и ценность
 3. Системная карта
 4. Экраны и задачи
 5. Архитектура и переиспользование
 6. Контракты и данные
 7. Подготовка и подтверждение
 8. Безопасность
 9. Отказы и сопровождение
 10. Развёртывание и статус
 11. Приёмка
 12. Открытые решения
- Разделение управляющих поверхностей

Область применения источника

Веб-Штурвал в составе Ядра — ограниченный интерфейс Core Operator API. Он читает состояние агента и предоставляет подготовку, подтверждение и чтение результата изменения имени, описания и языка. Публичная страница входа доступна.

Отдельный Operator MCP предоставляет разрешённые административные операции, а рабочее пространство Operator — фиксированный UI чтения. Это самостоятельные поверхности: их наличие не означает, что полный набор инструментов уже доступен в веб-Штурвале. Далее описан целевой состав и принципы; готовность каждой операции проверяется отдельно.

1. Цель и смысл

Помочь человеку понимать состояние ИИ-сотрудников, менять их настройки и сопровождать работу до результата. Оператор формулирует намерение, видит область и последствия изменения, подтверждает его и получает проверяемый результат. Это человеческая поверхность управления, доступная через браузер без Codex.

Штурвал использует существующие операции Operator и Core. Он не создаёт второй планировщик, память агентов или автономного администратора с неограниченными правами.

2. Пользователи и ценность

Оператор работает с назначенными агентами; системный администратор — с разрешёнными настройками экземпляра; аудитор читает доступный журнал. Эти роли не обязаны иметь доступ ко всем личным разговорам. Эффективная область показывается пользователю. Ценность: быстрее диагностировать проблему, применить нужное изменение и проверить его, сохранив непрерывность работы сотрудника. Метрики — время диагностики, подтверждённые результаты, конфликты/отказы и отсутствие дублированных действий.

3. Системная карта

```
flowchart LR
    Person[Оператор] --> Site[Сайт Штурвал]
    Site --> Auth[Сессия / роль / область]
    Auth --> Adapter[Серверный Operator adapter]
    Adapter --> Core[Core commands]
    Core --> Receipt[Status / receipt / события]
    Receipt --> Site
    Adapter --> Help[Приватная консультация через Core]
```

MCP — дополнительный транспорт/интерфейс интеграции. Пользователь не устанавливает MCP host. Серверная переиспользуемая логика и UI — разные части комплекта.

4. Экраны и задачи

Раздел	Что делает оператор	Область контроля
Обзор	Проверяет готовность и незавершённые задачи	Версия и время последней проверки
Агенты	Читает и меняет настройки/контекст/навыки	Agent scope, revision и diff

Раздел	Что делает оператор	Область контроля
Задания/диалоги	Диагностирует и консультируется	Разрешённое содержимое и выбранный разговор
Люди/доступ	Управляет назначениями при соответствующей роли	Отдельное полномочие, не роль любого оператора
Подключения	Настраивает модель/канал/коннектор	Metadata вместо раскрытия секрета
Устройства	Смотрит состояние и отзывает доступ	Назначенные устройства
Журнал/эксплуатация	Проверяет receipts, версии и recovery	Только свой экземпляр

Списки формируются по реальным capabilities Core. Неподдержанная операция не становится доступной из-за нарисованной кнопки. Существующие read endpoints нужно фильтровать по корпоративным ролям до показа содержимого.

5. Архитектура и переиспользование

Upstream источники: src/adapters/core.mjs, core-mcp-contract.mjs, operator-service.mjs. В Ядре: src/operator-access.ts, operator-http.ts, operator-agent-admin.ts, operator-message.ts, operator-consultation.ts и core-command.ts. Протоколы prepare/commit/status, digest, revision и receipts переиспользуются с тестами, а не заменяются прямыми изменениями файлов.

В текущем Operator есть прямой Core adapter без обязательного Master gateway. Персональные upstream auth-пути с Master не переносятся в контур заказчика. Company admin credential даёт широкую область; его скрывание за сайтом не создаёт персональный ACL. Нужен серверный контракт identity/scopes с проверкой в Core.

6. Контракты и данные

Read: access/capabilities, agent state/documents, conversations/context/reminders. Mutations: agent-changes/prepare и commit; messages/prepare и commit; status по ID. Consultation: start/read/cancel, отдельное применение/публикация результата. Точные private routes и ограничения: технический проект (см. оглавление документации).

Core хранит исходное намерение и бизнес-результат. Штурвал хранит серверную сессию, ссылки на операции и временный preview. Browser-переданный actor не считается доказательством личности. Защищённое сопоставление issuer/subject, роли и области обязательно; права перепроверяются при исполнении после ожидания.

7. Подготовка и подтверждение

Оператор выбирает объект → предлагает изменение → Core prepare нормализует действие → UI показывает адресата/diff/область/срок → пользователь подтверждает → Core проверяет actor, revision и digest → возвращает receipt. Устаревшее preview требует повторной подготовки. Таймаут после commit требует status, а не нового ID. Двойной клик возвращает тот же эффект/receipt. Новое содержание с тем же ID — конфликт.

Чат консультации помогает понять ситуацию. Сгенерированная рекомендация не является командой с повышенными правами. Приватный ответ не публикуется сотруднику сам.

8. Безопасность

Отдельный HTTPS origin, host-only cookie, OIDC, CSRF, проверка полномочий на сервере. Ключи Core/LLM в браузер не выдаются. Имена подключений и ошибки очищаются от секретов. IdP groups отображаются только на явно разрешённые роли. Истечение/отзыв сессии блокирует старое подтверждение. Доступ к чужой области запрещён и по прямому URL. Управление всем парком серверов поставщика и SSH/Fleet не входят в Штурвал Ядра.

9. Отказы и сопровождение

Core недоступен — операции не притворяются выполненными. Изменена revision — новый preview. Идёт другая операция — busy/conflict с понятным продолжением. Неизвестен внешний эффект — статус «требуется проверка». Перезапуск сайта не удаляет receipt. Журнал содержит actor, цель, время, intent/confirmation/result и связь с request; сроки хранения и экспорт определяются принятой политикой.

10. Развёртывание и статус

Сайт и backend на сервере заказчика, Core API только приватный. Проверенный срез Operator 0.2.12 содержит отдельный MCP и рабочее пространство; целевые тесты чтения, привязки компании и консультаций пройдены. Наличие этого кода не означает установку Operator у каждого пользователя. Требование Node $\geq 24.14.1$ < 25 относится к данному пакету. Веб-пилот чтения и settings prepare/commit развёрнут 11.09.2026. Полный scored authority, IdP и остальные операции целевого сайта ещё не приняты.

11. Приёмка

ENT-25/26/27/33 и DEMO-04/05/08: браузерный вход без внешнего чата; read по роли; подготовка/подтверждение; replay без дубля; private consultation; revoke; restart; отказ чужому actor; секреты не появляются в ответе, storage и безопасных логах.

12. Открытые решения

Делегированная identity, источники ролей, IdP, серверный transport Operator, проверка совместимости API и матрица функций первого релиза. Полный arbitrary Core API проху не считается подходящей реализацией этого контракта.

Общий контекст: системная карта (см. оглавление документации), критерии приёмки (см. оглавление документации), план демо (см. оглавление документации).

Разделение управляющих поверхностей

Веб-Штурвал нужен оператору компании в браузере. Operator MCP нужен авторизованному MCP-клиенту для чтений, подготовки и разрешённых действий Core. Рабочее пространство Operator показывает выбранные данные через ограниченный локальный интерфейс. Техническая страница Context в dashboard относится к лабораторному режиму владельца и не является готовым редактором ролей веб-Штурвала.

Административные права имеют область компании; произвольные роли подразделений и проектов этим не реализованы. Роль агента описывает его назначение, а права человека определяют доступ к действиям. Изменение текста роли агента не назначает пользователю новые полномочия.

Основание документа

Сверка продуктовых документов и закреплённых исходников 15 сентября 2026 года. Проверка документации не заменяет промышленную приёмку. Полная применимость определяется документом о состоянии компонентов.