

Модель безопасности и автономное размещение

Тимон Ядро · Служба информационной безопасности, архитектор, администратор

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

Границы доверия

Вход в веб пилот

Секреты и инструменты

Данные и знания

Подключение рабочего устройства

Работа без внешнего интернета

Проверка и ответственность

Управляемый Context и изоляция

Публичный чат

Границы доверия

Рабочий браузер, серверный backend, исполнитель модели, устройство сотрудника и внешний API рассматриваются как отдельные зоны. Документ, веб-страница и ответ модели являются входными данными. Они не предоставляют права на чтение чужой области, запуск команды или передачу сведений наружу.

Полномочия должны проверяться сервером для конкретного действия и объекта. Скрытая кнопка в интерфейсе не является механизмом защиты. После ожидания в очереди права необходимо учитывать повторно, поскольку доступ мог быть отозван. Полная корпоративная модель ролей остаётся предметом реализации и сквозной приёмки.

Вход в веб пилот

В пилоте используется отдельная сессия для каждого приложения. Cookie имеет признаки Secure, HttpOnly, SameSite Strict; изменения требуют проверки Origin и CSRF. Сеанс ограничен восемью часами и тридцатью минутами бездействия; перезапуск backend завершает сеансы в памяти. Изменение учётной записи или серверной привязки отзывает сессию.

Код доступа в этой конфигурации должен быть длинным и случайным. Описанная схема хранения его SHA-256 не предлагается как универсальная схема для коротких пользовательских паролей. Корпоративный IdP, MFA и жизненный цикл сотрудников требуют отдельной интеграции; наличие пилотного входа их не подтверждает.

Секреты и инструменты

Серверные ключи Core и модели не должны попадать в браузер, публичные материалы или обычные журналы. Конфигурация с секретами хранится вне каталога статического сайта. Контроль доступа распространяется и на процессы инструментов: сокрытие ключа в интерфейсе не доказывает, что его нельзя прочесть из дочернего процесса.

Для каждого инструмента определяют разрешённые файлы, сеть и операции. Подтверждение чувствительного действия должно относиться к конкретному содержанию, адресату и актуальному состоянию. Рекомендация модели не заменяет такое подтверждение. Изменение инструкции агента само по себе не расширяет системные полномочия.

Данные и знания

Для материалов задают владельца, область доступа, срок хранения и порядок удаления. Доступ к результату по прямой ссылке должен соответствовать доступу через интерфейс. Индекс, извлечённый текст и кеш требуют той же политики, что исходный материал. Отдельно проверяют доступ к историческим версиям и резервным копиям.

Вывод модели может содержать ошибку или воспроизвести недостоверные данные источника. Поэтому значимые решения сопровождаются проверяемыми ссылками и ответственным человеком. Политика базы знаний должна предусматривать исправление, замену и вывод устаревших правил из активного использования.

Подключение рабочего устройства

Штрих хранит личную работу сотрудника; Шлюз действует в браузере; Node обеспечивает транспорт и поддерживаемые локальные операции. У приложения и расширения разные области разрешений. Выбор вкладки не означает разрешение читать всю личную

библиотеку, а связь с корпоративным агентом не означает передачу всех материалов компании.

В проверенном кандидате связанная браузерная беседа ограничена профилем, сайтом и выбранным маршрутом. Проверяются совместимость транспорта, идентичность владельца, актуальность запроса остановки и сохранение черновика. Браузерный профиль не получает личную память и произвольные локальные инструменты только потому, что использует тот же установленный исполнитель.

Системные разрешения macOS, идентичность расширения и регистрация Native host проверяются отдельно. Windows-версия Штриха запланирована; наличие вспомогательного Windows-кода в Node не доказывает готовность приложения для Windows. При выпуске проверяются обновление и откат всего комплекта.

Работа без внешнего интернета

Автономность достигается конфигурацией: локальная модель, внутренние данные, доступные DNS и служба входа, локальные зависимости и разрешённые инструменты. Также необходимы работающие серверы, локальная сеть и питание. Интеграция с внешним сервисом без связи с ним не продолжит получать актуальные данные.

Приёмочный тест отключает внешний исходящий доступ и повторяет согласованные рабочие задачи, вход, работу с файлами и диагностику. Отдельно проверяют установку и обновление: способность уже запущенной системы работать офлайн не доказывает возможность установить её без сети. Внешний fallback должен быть исключён либо явно предусмотрен согласованной политикой.

Компания может пополнять знания и улучшать проверенные навыки в автономном режиме при наличии соответствующих локальных функций. Это не автоматическое дообучение весов модели. Изоляция сети также не является сама по себе сертификатом соответствия требованиям защиты информации.

Проверка и ответственность

План безопасности включает отрицательные тесты чужих объектов, отзыв сессий, прямые ссылки на файлы, утечки секретов, повторы действий, журналирование и восстановление. Результат привязывают к версии и среде. Проверка структуры кода и тесты на фикстурах не заменяют оценку промышленного контура.

Состав защитных мер и ответственность сторон фиксируются в проекте внедрения. Этот документ описывает модель и требования, не заявляет сертификацию, универсальную защищённость или готовность обработки любых категорий данных без оценки конкретной конфигурации.

Управляемый Context и изоляция

В свежем коде управляемый Context предназначен для коллекций знаний, пользовательских материалов, памяти и артефактов. Ролевая модель и области объектов должны ограничивать не только результат поиска, но и чтение исходного файла, старой версии, вложения и кеша.

Текущий режим выключен по умолчанию и предназначен для лабораторной работы владельца. При включённом лабораторном режиме либо наличии приватного vault выполняются защитные проверки перед запуском исполнителей других пользователей. Это предохранитель до завершения изоляции, а не готовая многопользовательская защита Context.

До выпуска требуется доказать, что инструменты процесса не читают чужие файлы в обход МСР. Разные каталоги, идентификаторы сессий и скрытая кнопка не обеспечивают такую границу сами по себе. Проверка API и локальных тестов не заменяет испытание операционной системы в конфигурации поставки.

Публичный чат

Публичный консультант использует отдельный профиль OpenCode с запрещёнными инструментами. Его гостевая история и разрешённая документация отделены от корпоративных пользователей и агентов. В браузере ответы отображаются как текст; только точные ссылки из разрешённого каталога превращаются в иллюстрации.

Гостя определяет серверная cookie; идентификатор другого пользователя, указанный в сообщении, не выбирает чужую историю. Согласие на обработку данных и карточка провайдера доступны до отправки. На общем профиле браузера история принадлежит этому профилю, поэтому общий компьютер требует своей политики использования.

Такая изоляция публичного помощника не подтверждает автоматически изоляцию всех корпоративных исполнителей, клиентских МСР и систем компании. Применимость каждой меры проверяется в её собственном контуре.

Основание документа

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