ЭКСПЛУАТАЦИЯ СЕРВЕРА

Руководство администратора

Продукт: СОПКА.Рой · Версия: 1.0.0 · Агент: 1.0.1 · Протокол: 1 · Редакция: 15.10.2026

Правообладатель ПО: Общество с ограниченной ответственностью «Каннам». ИНН 2543020645, ОГРН 1132543001502. Реквизиты приведены в отдельном разделе документации.

Первичная настройка

1. Скопируйте `.env.example` в `.env` и замените все демонстрационные секреты.
2. В production один раз задайте канонический адрес вместе с путём: `COPKA_ROY_PUBLIC_URL=https://servername.com/roy`. Это условный адрес: замените домен и префикс на адрес своей установки. Из канонического адреса выводятся base path, CORS и Socket.IO origin.
3. Настройте отдельные пароли PostgreSQL для суперпользователя, мигратора и приложения.
4. В production включите обязательные серверные службы, строгий pre-auth rate limit и внешний HTTPS.
5. Запустите Docker Compose и проверьте локальные служебные пробы готовности.

Роли рабочей области

Роль	Назначение
admin	Управление рабочей областью, пользователями, политиками, агентами и чувствительными удалёнными функциями.
editor	Просмотр и изменение рабочих данных, политик и инцидентов без полного административного доступа.
viewer	Просмотр разрешённых данных без изменения конфигурации.

Настройки хранения

В интерфейсе рабочей области задаются сроки хранения событий, инцидентов и снимков. Текущие пределы формы: события - до 180 дней, инциденты - до 360 дней; значение для снимков задаётся отдельно. Администратор обязан согласовать сроки с политикой организации и доступным объёмом диска.

Резервное копирование и восстановление

Согласуйте допустимую потерю данных и время восстановления. Комплект копии включает PostgreSQL, историю ClickHouse, объекты RustFS/S3, конфигурацию и ключи. Состояние серверных служб резервируется согласно принятой схеме, но не заменяет постоянные данные. Дамп одной PostgreSQL недостаточен для восстановления журналов и снимков.

1. Ограничьте запись на согласованное окно или используйте согласованную схему снимков хранилищ.
2. Сохраните схему и данные PostgreSQL, конфигурацию/данные ClickHouse и содержимое S3-бакетов средствами соответствующих хранилищ.
3. Отдельно защитите .env, ключи подписи и информацию о версиях приложения и миграций; не включайте секреты в открытые архивы поддержки.
4. Восстановите копии в изолированном стенде без доступа рабочих агентов.
5. Проверьте вход, workspace, журналы, инциденты и открытие нескольких бинарных материалов.

Временные удалённые сеансы не следует считать восстановленными вместе с копией. Срок хранения копий и доступ к ним задаются отдельно от сроков хранения данных в интерфейсе.

Установка и обновление агентов

Администратор создаёт регистрационный ключ в разделе «Установка агента», скачивает EXE-установщик и передаёт на рабочую станцию только ключ и команду запуска. Интерфейс показывает полный ключ один раз, затем хранит и отображает только preview.

Обновления агентов управляются режимом `COPKA_ROY_AGENT_UPDATE_MODE`. В режиме `auto` сервер сам ставит устаревших клиентов в очередь, в режиме `manual` очередь запускается администратором, в режиме `off` обновления не предлагаются через heartbeat. Режим выбирается при внедрении и фиксируется регламентом сопровождения.

Переменная `COPKA_ROY_AGENT_UPDATE_ROLLOUT_PERCENT` задаёт глобальный процент охвата по умолчанию; текущее значение рабочей области отображается рядом с версией релиза. Владелец инсталляции может менять процент от 1 до 100 через Owner API. Кнопка «Остановить обновления» прекращает выдачу новых пакетов и отменяет только ожидающие задания; начатые скачивания и установки завершаются.

Контроль состояния

Проверка	Адрес или команда
Локальная проверка процесса	`/roy/api/health/live`, доступ из локальной сети или с reverse proxy.
Локальная проверка готовности	`/roy/api/health/ready`, используется для контейнера и внутреннего мониторинга.
Контейнеры	`docker compose ps`
Логи приложения	`docker compose logs -f app`

Журналирование

Сервер ведёт структурированные журналы, аудит операций пользователей и историю инцидентов. Доступ к журналам ограничивается ролью, а экспортируемые материалы должны очищаться от токенов и секретов.

Пользователи, приглашения и почта

Перед приглашением выберите рабочую область и минимально необходимую роль. После принятия проверьте членство именно в нужной области. Для отправки приглашений настройте SMTP: сервер, порт, режим TLS, учётную запись и адрес отправителя. Не отключайте проверку сертификатов для обхода ошибки почты.

Наблюдение за инфраструктурой

Контролируйте доступность PostgreSQL, ClickHouse, серверные службы, S3, task-worker и обратного прокси, свободное место и рост очередей. При отсутствии новых событий сравните приём агентских запросов с доставкой outbox. При ошибке открытия материала отдельно проверяйте metadata в БД и наличие объекта в S3.

Grafana предназначена для разрешённого административного доступа. Показатели «Компании» относятся к workspace; фильтр компании не является границей доступа. При отсутствии истории панель не доказывает нулевую активность: проверьте время последнего сбора.

Реагирование на сбой

1. Зафиксируйте время, workspace, клиента и точный симптом.
2. Проверьте readiness, состояние контейнеров, диска и зависимостей.
3. Сопоставьте логи приложения, worker и соответствующего хранилища.

4. Не удаляйте volumes, outbox, evidence или миграционные отметки для «быстрого» восстановления.
5. После устранения причины подтвердите поступление тестового события и доступ к старому материалу.

API рабочей области

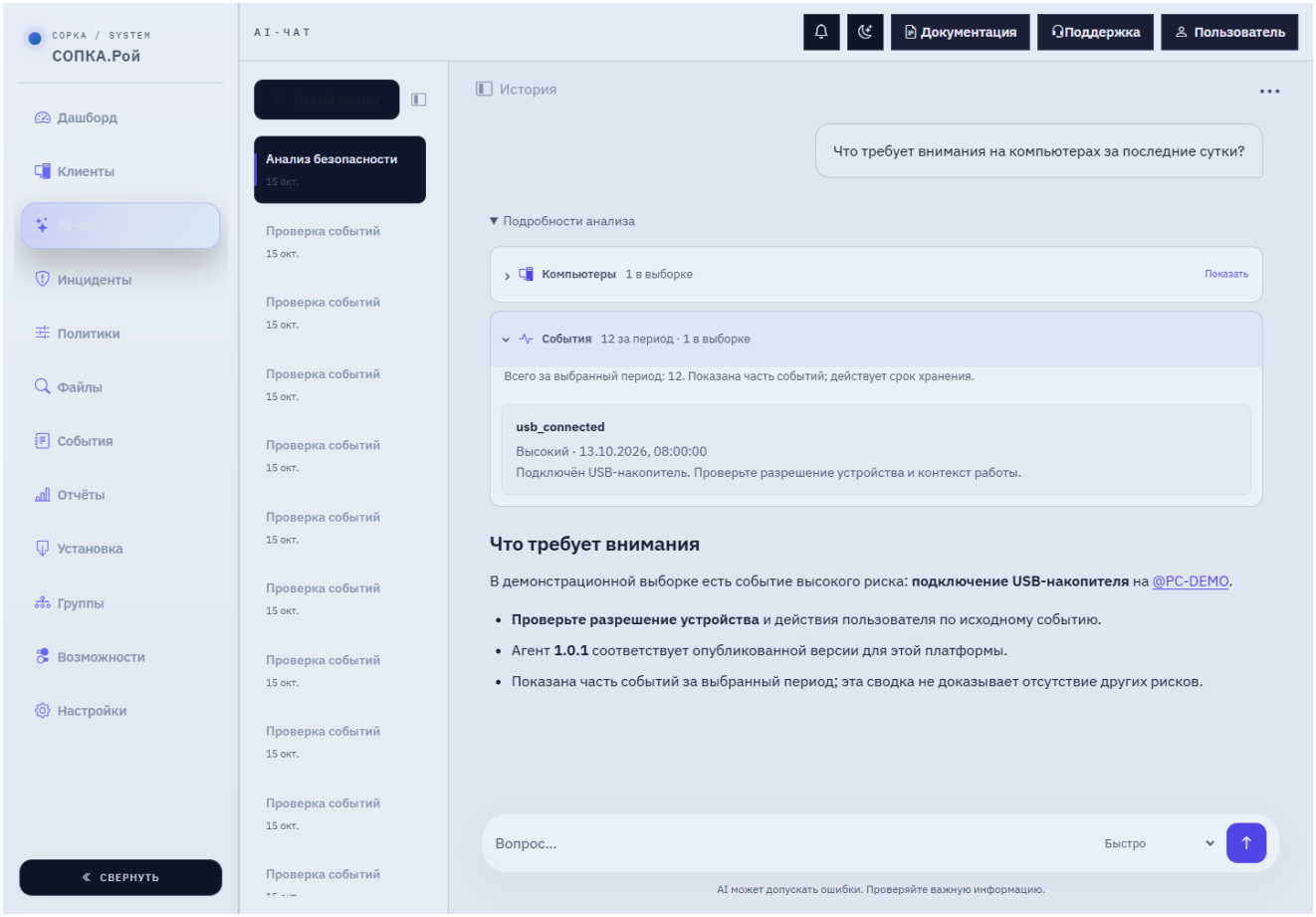
В разработке. Не включайте COPKA_ROY_WORKSPACE_API_ENABLED для рабочих интеграций на основании наличия маршрутов: контракт пока нестабилен. Тестирование выполняется в отдельной рабочей области на стенде.

Планирование нагрузки и изменений

Используйте единый расчёт из «Системных требований»: 1000 активных агентов, частота событий, интервал и размер снимков, срок хранения и параллельная работа операторов. Изменение интервала снимков, состава функций, массовое обновление и рост истории требуют пересчёта. Для начала работ проверяют фактические ресурсы хоста, лимиты контейнеров, пулы подключений, запас очереди и доступную ёмкость объектов. Сохранение политики не отменяет уже выполненные действия; восстановление доступа выполняется отдельной разрешённой операцией.

Доступ к AI-анализу

Диалоги принадлежат пользователю в выбранной рабочей области. Администратор не получает доступ к чужим чатам через этот интерфейс. Набор инструментов зависит от прав на соответствующие разделы. При временной недоступности сервиса история сохраняется; конфигурацию внешнего AI-сервиса и общие квоты подготавливает оператор развёртывания.



Подробнее: AI-чат: анализ безопасности.