МОДЕЛЬ ЗАЩИТЫ

Безопасность

Продукт: СОПКА.Рой · Версия: 1.0.0 · Агент: 1.0.0 · Протокол: 1 · Редакция: 14.08.2026

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

Контур эксплуатации

СОПКА.Рой рассчитана на локальное или выделенное развёртывание по договору. Сервер размещается в инфраструктуре заказчика или в согласованном защищённом контуре. Доступ пользователей, состав включённых модулей контроля, сроки хранения и порядок реагирования определяются договором, локальными актами и ролями рабочей области.

Сервер приложения публикуется через reverse proxy по HTTPS. PostgreSQL, Redis и служебные endpoints не предназначены для прямой публикации в Интернет. Проверки `/roy/api/health/live` и `/roy/api/health/ready` используются для локального мониторинга контейнера и reverse proxy.

Разграничение доступа

Данные клиентов, событий, инцидентов, политик и заданий относятся к рабочей области. Пользователь получает доступ только к тем рабочим областям, где он является участником. Роли `admin`, `editor` и `viewer` ограничивают управление пользователями, политиками, клиентами, расследованиями и настройками.

Проверка рабочей области выполняется на сервере. Идентификаторы, переданные из формы или JSON, не считаются основанием доступа без проверки роли пользователя или валидного агентского секрета.

Регистрация агента

Windows-агент регистрируется по регистрационному ключу. Ключ привязан к рабочей области, действует ограниченное время и после создания показывается полностью только один раз. В дальнейшем интерфейс отображает preview, чтобы администратор мог сверить начало и конец ключа без раскрытия полного секрета.

После регистрации агент получает device-токен. Этот токен используется для heartbeat, получения политик, отправки событий, статусов команд и запросов обновления. При отзыве регистрации сервер прекращает принимать новые запросы от соответствующего клиента.

Подпись политик и обновлений

Bundle политик подписывается Ed25519. Агент проверяет подпись и версию протокола до применения правил. Это защищает клиент от применения неподписанного или несовместимого набора политик.

Пакет обновления агента содержит манифест, SHA-256 файлов и подпись Ed25519. `CopkaRoyUpdater.exe` проверяет манифест и контрольные суммы до переключения версии. Обновление применяется через версионные слоты; при неуспешном запуске службы возможен откат.

Интерактивные каналы

Прямой экран и удалённый PowerShell являются интерактивными функциями и запускаются только по явной команде пользователя с соответствующей ролью. Их нельзя считать фоновым постоянным мониторингом: сеанс должен быть инициирован, завершён и отражён в журнале действий.

Обмен временными сообщениями интерактивных каналов защищается отдельными сессионными ключами. Для прямого экрана агент и браузер согласуют ключ через ECDH P-256, производят ключевой материал через HKDF и шифруют кадры AES-GCM с 12-байтовым nonce и привязкой к идентификатору сессии. Сервер передаёт зашифрованный поток и служебные метаданные, но не должен иметь открытый текст кадра.

Удалённый PowerShell использует алгоритм `ecdh-p256-hkdf-sha256-aes-256-gcm`. Браузер и пользовательский агент выводят два независимых ключа AES-256-GCM: один для ввода оператора, второй для вывода консоли. В AES-GCM используется 12-байтовый nonce и additional authenticated data с идентификатором сессии, направлением и порядковым номером сообщения. Ключи таких сессий являются временными. При отсутствии подготовленного ключа live-screen или shell-сеанс не должен деградировать в открытый режим, а должен завершаться ошибкой. В production при недоступности Redis интерактивные каналы также должны завершаться безопасной ошибкой, потому что Redis участвует в оперативном обмене и состоянии сессий.

Хранение и журналы

События, инциденты, статусы команд, результаты поиска файлов и служебные журналы хранятся в соответствии с настройками рабочей области и регламентом заказчика. Секреты, токены, регистрационные ключи, cookie и авторизационные заголовки не должны попадать в журналы в открытом виде.

Снимки экрана, прямой экран, клавиатурные события, буфер обмена и загрузка файлов относятся к чувствительным функциям. Их использование должно быть разрешено политикой организации, отражено в локальных документах и ограничено кругом уполномоченных пользователей.

Сетевой периметр

• публикуется только HTTPS reverse proxy с маршрутом `/roy`;

• служебные проверки готовности доступны из локальной сети или с reverse proxy;

- PostgreSQL и Redis остаются во внутренней Docker-сети;
- WebSocket upgrade разрешается только для маршрутов продукта;
- резервное копирование и восстановление проверяются до ввода в эксплуатацию.