

РУКОВОДСТВО ПО AI-АНАЛИТИКУ

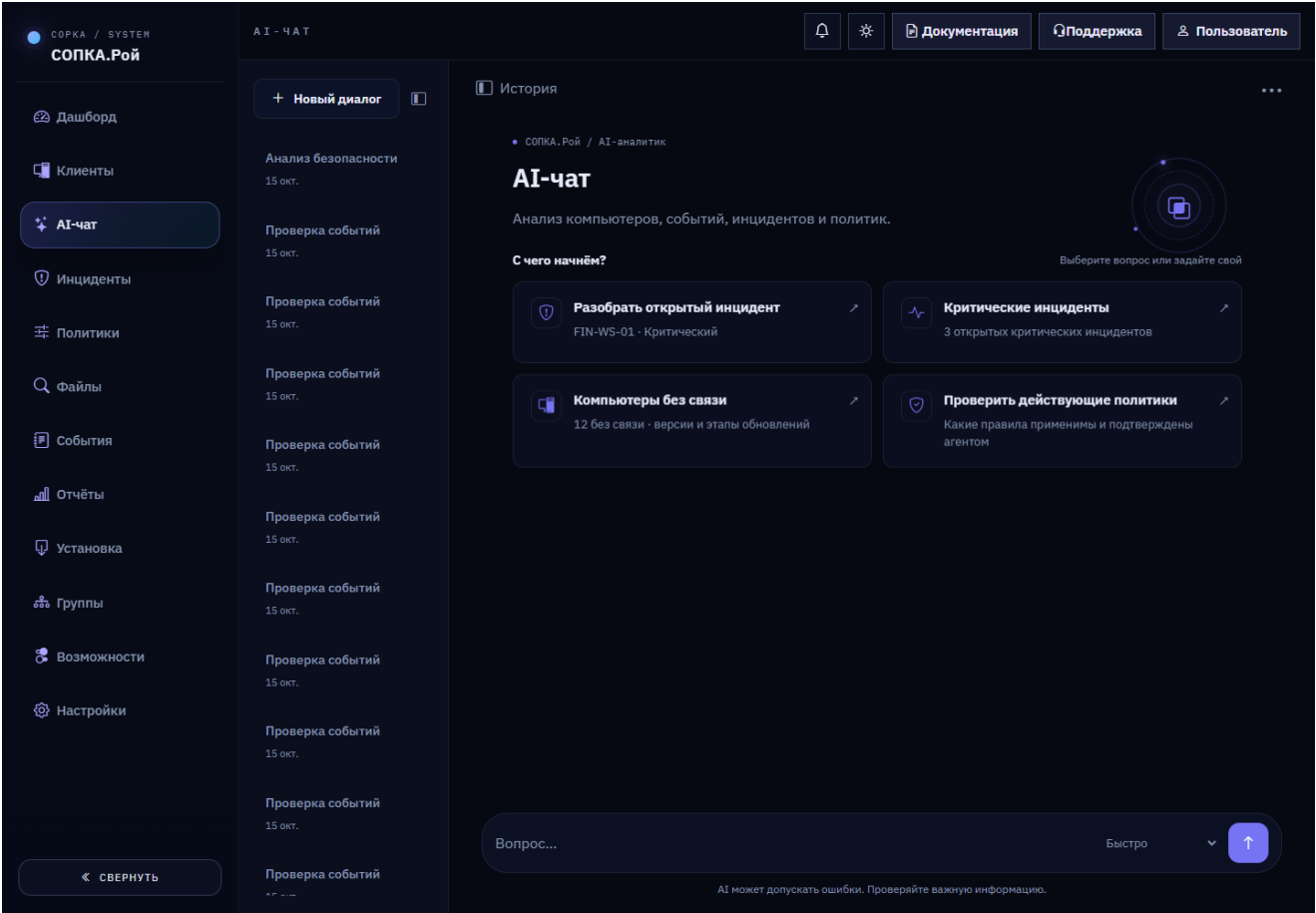
AI-чат: анализ безопасности

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.

AI-чат

Помощник анализирует компьютеры, события, инциденты, группы, политики, возможности, историю команд и результаты поиска файлов выбранной рабочей области. Откройте «AI-чат» в меню. Диалоги личные: другие участники не видят их через интерфейс чата.



Как задать вопрос

1. Проверьте выбранную рабочую область.

2. Нажмите «Новый диалог» или откройте историю.
3. Укажите цель, компьютер и период: «Разбери инциденты высокого риска за сутки» или «Проверь все компьютеры».
4. Выберите глубину анализа. Enter отправляет вопрос, Shift+Enter переносит строку.
5. Сопоставьте вывод с подробностями анализа и исходными карточками.

Приветствия, вопросы о возможностях помощника и о том, как пользоваться СОПКА.Рой, допустимы. Посторонние темы получают ответ «Извините. Мы не можем обработать данный запрос».

Упоминания и ссылки

Введите @ и выберите компьютер, группу, политику или инцидент. Упоминание задаёт конкретный объект. Проверенные названия объектов в ответе отображаются ссылками с @: нажатие открывает карточку. Одинаковые названия разных объектов не связываются автоматически без однозначного соответствия.

Что можно проверить

Данные	Возможности анализа
Рабочая область и дашборд	Лимит компьютеров, использованные и свободные места, агрегаты событий, инцидентов и состояния агентов.
Компьютеры	Поиск конкретного компьютера, сведения о системе и дисках, группы, наблюдаемые настройки безопасности, версии и этапы обновления.
Общая проверка	Связь, версии и обновления всех действующих компьютеров одним вызовом без страниц. Примеры проблем ограничены, общие числа относятся ко всему списку. Проверка не доказывает безопасность всей ОС и содержимого файлов.
События и инциденты	События по времени, важности и компьютеру; карточка инцидента, связанные события, комментарии, история расследования и ответственный.

Данные	Возможности анализа
Группы и политики	Состав групп, правила и область применения политик, действующие политики компьютера и подтверждения их доставки службой и пользовательским агентом.
Возможности и команды	Каталог возможностей, итоговые настройки компьютера и история команд. Отсутствие подтверждения не означает успешное выполнение.
Файлы и задачи	Уже найденные файлы и состояния задач поиска. Анализ не запускает новое сканирование и не читает содержимое файлов.
Документация и интернет	Справка СОПКА.Рой и публичные источники по безопасности.

СОПКА / SYSTEM
СОПКА.Рой

Дашборд

Клиенты

AI-чат

Инциденты

Политики

Файлы

События

Отчёты

Установка

Группы

Возможности

Настройки

← СВЕРНУТЬ

AI-ЧАТ

+ Новый диалог

Анализ безопасности
15 окт.

Проверка событий
15 окт.

Проверка событий
15 окт.

Проверка событий
15 окт.

Проверка событий
15 окт.

Проверка событий
15 окт.

Проверка событий
15 окт.

Проверка событий
15 окт.

Проверка событий
15 окт.

Проверка событий
15 окт.

Проверка событий
15 окт.

История

Что требует внимания на компьютерах за последние сутки?

▼ Подробности анализа

Компьютеры 1 в выборке

Показать

▼ События 12 за период · 1 в выборке

Всего за выбранный период: 12. Показана часть событий; действует срок хранения.

usb_connected

Высокий · 13.10.2026, 08:00:00

Подключён USB-накопитель. Проверьте разрешение устройства и контекст работы.

Что требует внимания

В демонстрационной выборке есть событие высокого риска: подключение USB-накопителя на @PC-DEMO.

- Проверьте разрешение устройства и действия пользователя по исходному событию.
- Агент 1.0.1 соответствует опубликованной версии для этой платформы.
- Показана часть событий за выбранный период; эта сводка не доказывает отсутствие других рисков.

Вопрос...

Быстро

↑

AI может допускать ошибки. Проверьте важную информацию.

Команды через AI

Попросите «Синхронизируй политики на @компьютере» или «Перезагрузи все компьютеры группы». Помощник готовит карточку подтверждения под ответом. Подробности анализа остаются сверху. До нажатия «Выполнить» команды не отправляются.

- Синхронизация политик.
- Обновление инвентаря.
- Штатная проверка обновления агента; установка зависит от настроек рабочей области.
- Перезагрузка и выключение с задержкой 30 секунд после выполнения команды агентом.
- Завершение сеанса пользователя.
- Отмена отложенного выключения или перезагрузки.

Для питания требуется разрешённая возможность управления питанием; перезагрузка, выключение и выход могут привести к потере несохранённых данных. Доступ также зависит от прав пользователя. Аналитик не изменяет политики и не выполняет произвольные команды.

Массовый запуск

Выберите компьютеры, одну группу или всю область — до 200 компьютеров за запуск. Карточка показывает общие числа доступных и пропущенных, без перечисления всех клиентов.

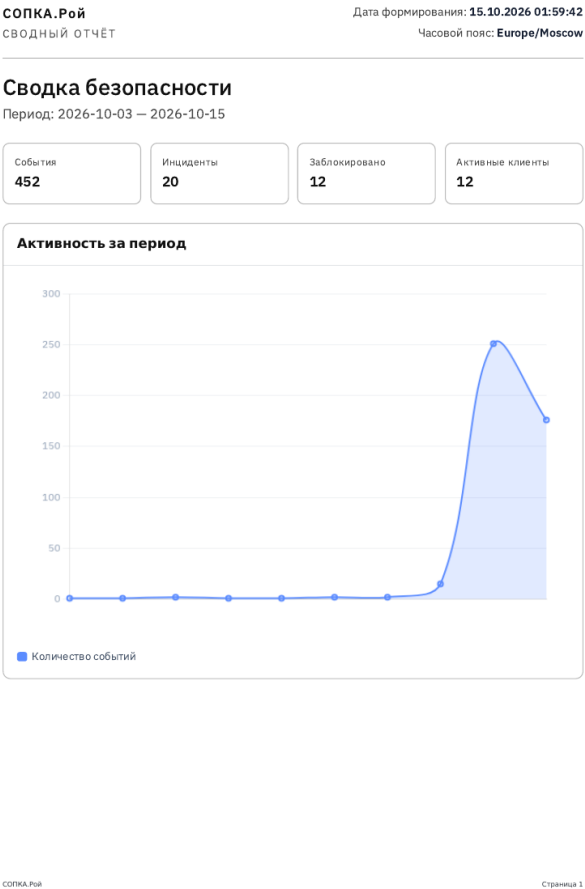
Отключённые компьютеры пропускаются. Состав целей фиксируется при подготовке; связь, права и возможности повторно проверяются перед отправкой.

Подтверждение действует 10 минут, привязано к пользователю и области и используется один раз. Очередь, подтверждение получения и завершение — разные состояния. Массовая команда ожидает подтверждения получения агентом до 30 секунд, затем истекает и не выдаётся при последующем включении ПК. Уже выполняющаяся команда использует свой обычный таймаут. Истёкшие команды автоматически не отправляются заново; фактический результат доступен в истории команд.

PDF-отчёты и скачивание

Например: «Сформируй PDF-отчёт по агентам за неделю». Используются те же данные, шаблон, шрифты, графики и таблицы, что в разделе «Отчёты». Доступны обзор, инциденты, политики, блокировки, компьютеры, агенты, типы событий, устройства и файлы. Можно задать период, компьютер или группу.

В ответе появляется прямая ссылка «Скачать PDF» и ссылка в карточке файла. Для скачивания нужен вход под аккаунтом автора и выбранная рабочая область. Серверная копия доступна 24 часа с создания. Затем ссылка сообщает об истечении срока, а ближайшая фоновая очистка удаляет файл. Создайте отчёт заново, если срок истёк.



СОПКА.Рой

Страница 1

Источники и достоверность

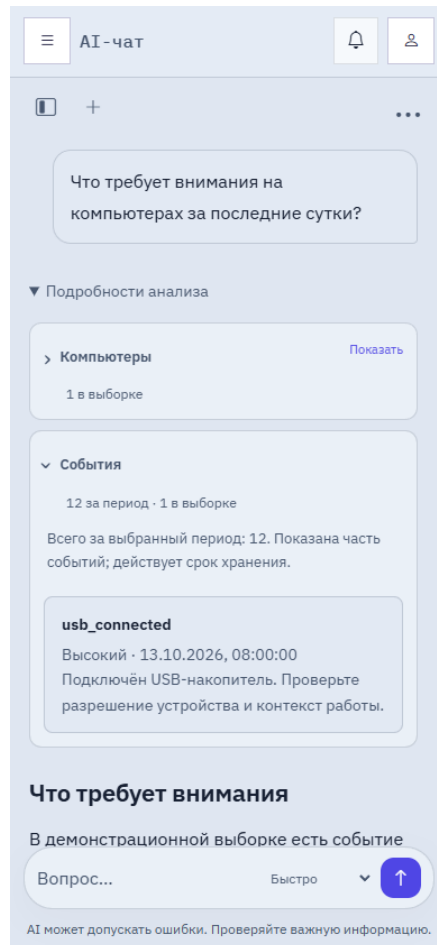
Версии сравниваются с опубликованными релизами сервера для платформы и архитектуры. Неизвестный целевой релиз не означает, что агент устарел. Подтверждение доставки политики отличается от её применимости. Ограниченный список событий не равен всей истории.

При необходимости помощник сам выбирает интернет-поиск. В подробностях видно запрос и источники. Для справки о процессе можно указать имя исполняемого файла; оно само по себе не доказывает заражение. В публичный поиск не отправляются внутренние имена компьютеров, IP, пути и тексты событий.

Вопрос и ограниченные результаты анализа передаются настроенному внешнему AI-сервису. Не включайте пароли, ключи и персональные переписки. Данные событий и внешних источников не считаются инструкциями; права проверяет сервер независимо от текста запроса. Ответы AI могут содержать ошибки — проверяйте важные выводы.

История, прокрутка и мобильный экран

Историю можно скрыть кнопкой «История». На телефоне она открывается выдвигной панелью с кнопкой закрытия. Новые сообщения не принуждают к прокрутке; кнопка перехода к последнему сообщению появляется, когда вы находитесь выше. После завершения ответа это стрелка вниз. Действия с диалогом находятся в меню с тремя точками.



Если ответ не получен

- При квоте сообщение «Лимит AI исчерпан. Попробуйте позже» отображается вместо вопроса в поле ввода. Удаление или создание диалога не сбрасывает серверный лимит.
- Кнопка «Повторить запрос» восстанавливает исходный вопрос и заново проверяет доступность.
- При временной недоступности AI история сохраняется.
- Если инструмент недоступен, проверьте права и выбранную область.
- Прерванный ответ может содержать частичные результаты. Проверяйте их ограничения.