РУКОВОДСТВО ПО AI-АНАЛИТИКУ

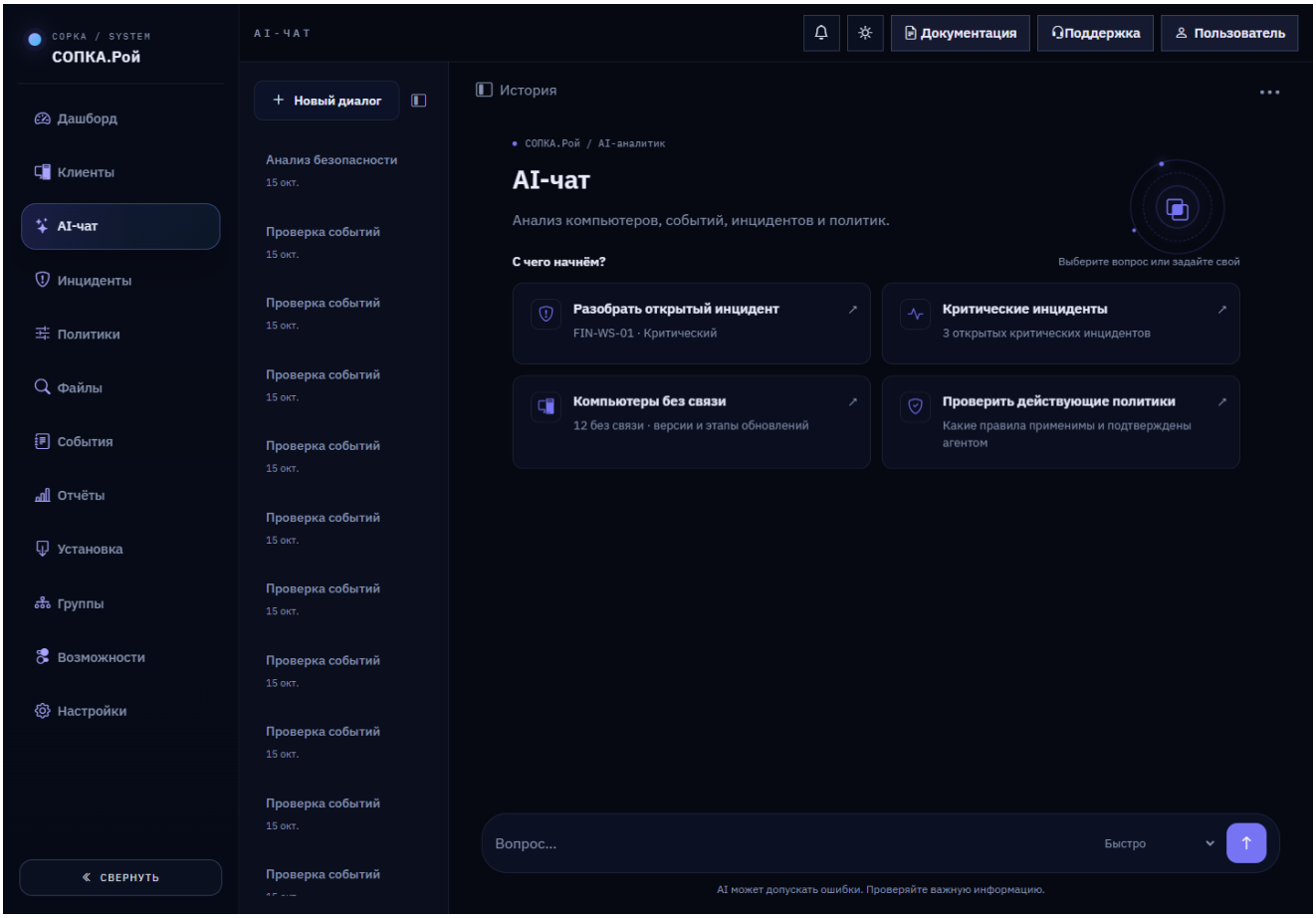
AI-чат: анализ безопасности

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 исходными карточками и указанными источниками.

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

Файлы и буфер обмена

Прикрепите файл кнопкой «+», перетащите его в чат или вставьте изображение из буфера обмена. Перед отправкой проверьте список вложений и удалите лишние. Можно передавать текст, исходный код, CSV, PDF и изображения PNG, JPEG, WebP, GIF. Прикреплённое содержимое передаётся настроенному AI-сервису для анализа вместе с вопросом; код из вложения не запускается.

За запрос допускается до трёх файлов: каждый не больше 5 МиБ, суммарно до 12 МиБ. PDF — до 20 страниц; изображения и страницы скана — не более пяти на запрос. Объём извлечённого текста ограничен 16 000 байтами UTF-8 на запрос. Если передана только часть, вложение помечается соответствующим образом; вывод относится к этой части. Сократите документ или разделите его на несколько запросов.

Вопрос и вложения доступны автору в текущей рабочей области. Не отправляйте секреты, которые нельзя передавать используемому AI-сервису. Текст документа рассматривается как данные, а не разрешение на выполнение команд.

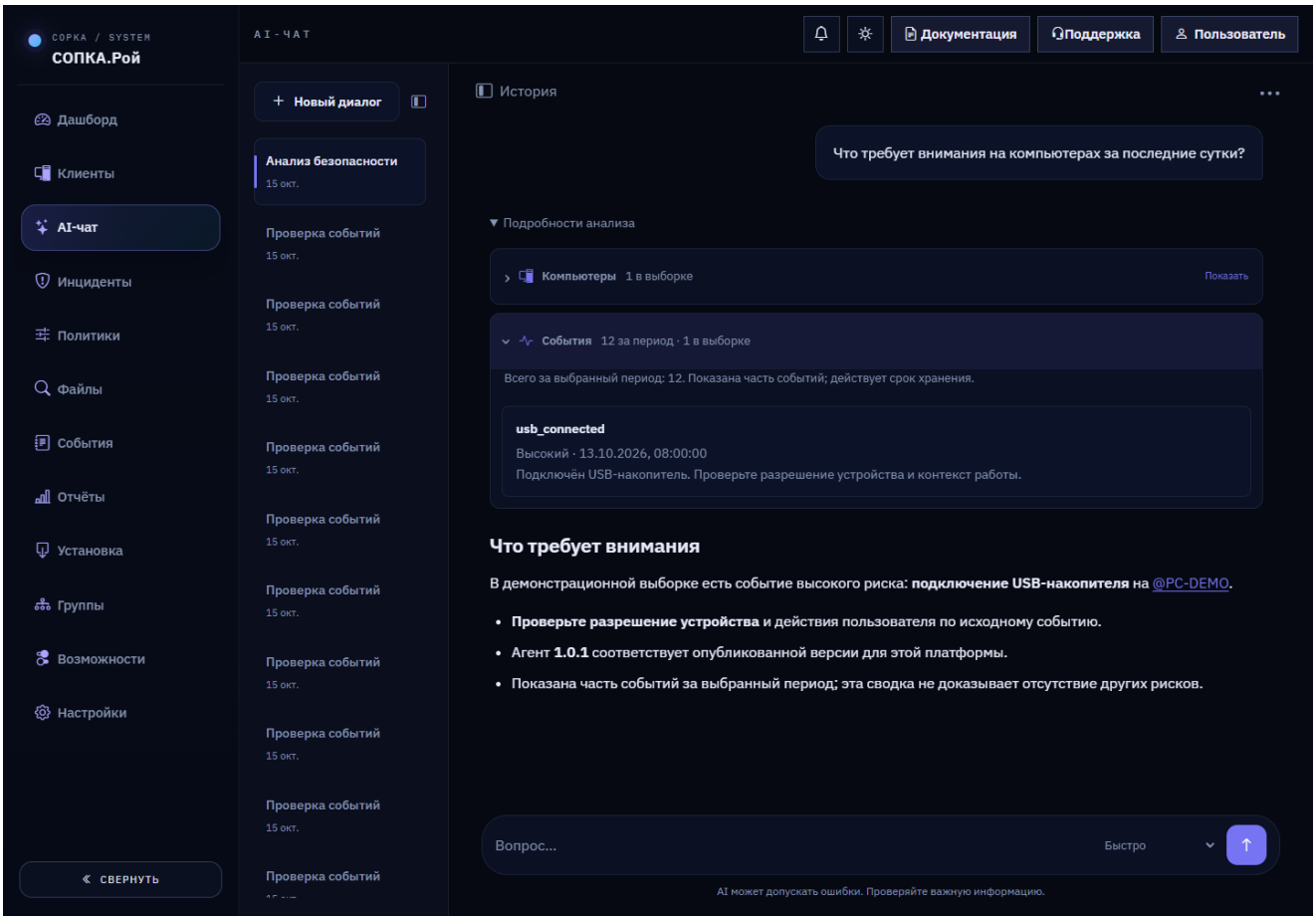
Упоминания и ссылки

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.

Данные	Возможности анализа
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.
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.



Команды через AI

Попросите «Синхронизируй политики на @компьютере» или «Перезагрузи все компьютеры группы». Помощник готовит карточку подтверждения под ответом. Во время обработки показывается короткий статус текущего действия; внутренние рассуждения модели не раскрываются. 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

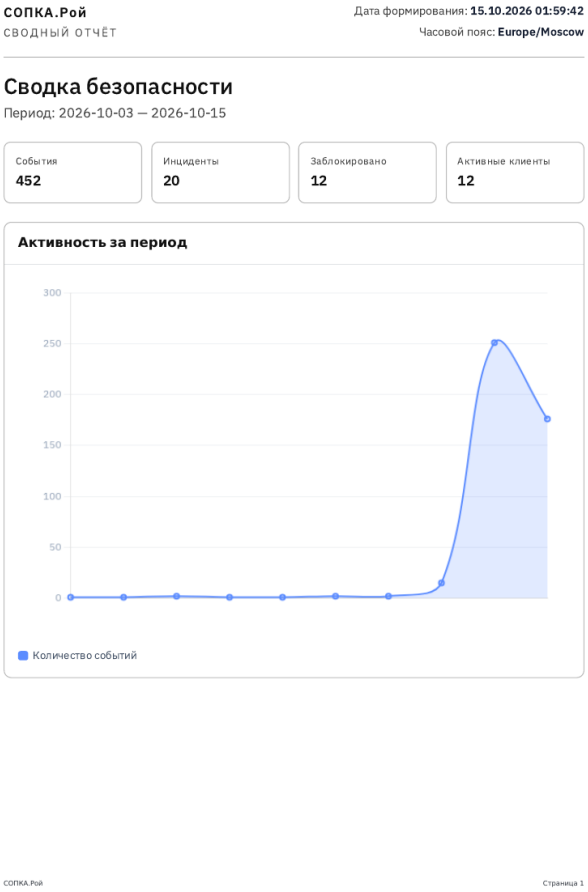
Выберите компьютеры, одну группу или всю область — до 200 компьютеров за запуск. Карточка показывает общие числа доступных и пропущенных, без перечисления всех клиентов. Отключённые компьютеры пропускаются. Состав целей фиксируется при подготовке; связь, права и возможности повторно проверяются перед 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. Итог массового запуска показывается в чате и уведомлении с названием команды и количеством результатов. Отсутствие подтверждения не считается успехом.

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.



Источники и достоверность

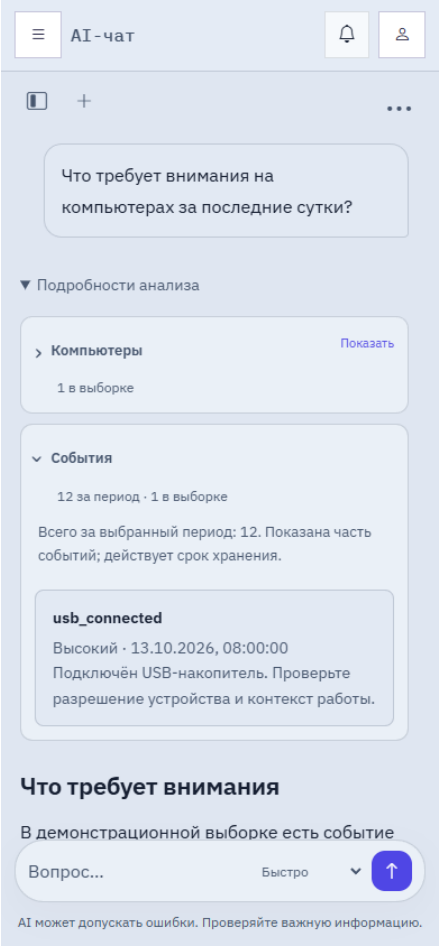
Версии сравниваются с опубликованными релизами сервера для платформы и архитектуры. Неизвестный целевой релиз не означает, что агент устарел. Подтверждение доставки политики отличается от её применимости. Ограниченный список событий не равен всей истории.

При необходимости помощник сам выбирает интернет-поиск. Текущий статус поясняет выполняемое действие: поиск данных, поиск в интернете или открытие источника. 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 выдвижной панелью с кнопкой закрытия. После отправки ваш новый вопрос поднимается в область чтения. Поток ответа не прокручивает страницу за каждым фрагментом; кнопка перехода к последнему сообщению появляется, когда вы находитесь выше. После завершения ответа это стрелка вниз. Для удаления диалога используйте значок корзины в истории.



Срок хранения и формат ответов

История сгруппирована по времени: «Сегодня», «Вчера», «Последние 7 дней», «Последние 30 дней», далее по месяцам. Диалог без обновления более 90 дней удаляется при очистке неактивной истории. Открытие старого чата само по себе не гарантирует продление срока. Удалённую переписку нельзя восстановить через интерфейс.

Ответ появляется постепенно по мере поступления текста. Поддерживаются Markdown, списки, таблицы и блоки кода с обозначением языка и копированием. Код в ответе — текст для проверки пользователем; его показ не означает выполнение на компьютере.

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.