РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Файлы, маркировки и шаблоны

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.

Поиск файлов и маркировки

Раздел «Файлы» объединяет задания поиска, результаты, помеченные файлы, маркировки и передачи. Задание задаёт условия проверки на выбранных компьютерах; результаты появляются после выполнения агентом. Инструкция актуализирована 11 ноября 2026 года.

Создание задания

1. Откройте «Файлы → Поиск» и создайте задание.
2. Укажите название и область действия: компьютеры или группы. Проверьте, включены ли будущие клиенты.
3. Добавьте ручные условия либо примените шаблон библиотеки. Условия могут проверять имя, путь и содержимое; выберите нужное сочетание AND / OR.
4. Сохраните задание и запустите поиск. Проверьте доступность компьютеров и поддержку условий агентом.
5. Откройте результаты и карточку нужного файла.

В списке заданий показывается последний запуск: например, «№2: Завершено», «№3: Выполняется» или состояние ошибки. Цвет помогает различать состояния. «Не запускался» означает, что запусков ещё нет. Подробности задания содержат дополнительные сведения о запуске; завершение поиска не подтверждает отсутствие чувствительных данных вне заданной области.

Шаблоны рабочей области и PCRE2

Библиотека находится в «Настройки → Шаблоны». Здесь можно искать встроенные и собственные шаблоны, создавать и редактировать свои выражения, загружать их из TXT. Собственные шаблоны принадлежат текущей рабочей области и доступны в поиске файлов и редакторе DLP-политик. Ручной ввод условий остаётся доступен.

Собственные регулярные выражения используют PCRE2 — синтаксис режима PCRE2 на regex101. Проверка выполняется сервером, а выполнение на компьютере требует версии агента с поддержкой PCRE2. Ошибку проверки нужно исправить до сохранения; несовместимый агент следует обновить. Не переносите специфические конструкции Python `re` без проверки совместимости.

Применение собственного шаблона копирует его выражение в правило. Последующее изменение или удаление шаблона не переписывает уже сохранённые правила: откройте правило и примените новую версию отдельно.

Встроенный шаблон	Что проверяет
Паспорт РФ	Формат серии и номера, без проверки выдачи документа.
СНИЛС и ИНН	Формат и контрольные цифры.
Банковские карты	Числовой формат и контрольная сумма Luhn.
IBAN	Структура и MOD 97, без подтверждения существования счёта.
API-ключи и токены	Известные префиксы и структуры; действительность секрета не проверяется.
Файлы .env	Имя файла, включая .env.*; имя не доказывает наличие секрета.
Секреты конфигурации и приватные ключи	Характерные присваивания и заголовки ключевого материала.

Совпадение — основание для проверки. Оно не подтверждает подлинность документа, активность карты или действительность ключа. Проверки контрольных сумм относятся к встроенным детекторам; произвольное регулярное выражение не получает их автоматически.

Найденные и помеченные файлы

В колонке обнаружения показывается дата первого обнаружения. Дата последнего обнаружения находится в подробностях. Для получения полного содержимого или скачивания требуются соответствующие права и доступность функции у агента; наличие записи в таблице не означает, что файл уже скачан на сервер.

Нажмите строку помеченного файла, чтобы открыть сведения: путь, компьютер, размер, первое и последнее обнаружение, теги и SHA-256. В этом же окне доступны переход в карточку, просмотр текста и скачивание — в пределах ваших прав. Теги и хеш сохранены в подробностях, но не занимают отдельные колонки списка.

Создание и применение маркировки

1. Откройте вкладку «Маркировки» и нажмите «Добавить маркировку».
2. На отдельной странице задайте название, цвет и необязательное краткое описание. Сохраните.
3. В карточке найденного файла выберите маркировку и примените её.
4. Используйте вкладку «Помеченные» для просмотра отмеченных файлов и фильтрации.

Карточки маркировок оформлены как группы. Справа отображается количество связанных файлов без отметки удаления. Поиск помогает найти маркировку по названию или описанию; редактирование открывается на отдельной странице. Цвет метки одинаков в списке и карточках файлов.

Если результатов нет

• Проверьте область поиска, условия и фактическое состояние последнего запуска.

• Убедитесь, что клиент на связи и поддерживает используемые шаблоны.

• Проверьте фильтры и период; пустая таблица сама по себе не означает успешное сканирование.

• Если текст недоступен, проверьте права, формат файла и состояние передачи.