RULE ENGINE

Политики и каналы контроля

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.

Политика, возможность и событие

Возможность разрешает функцию агента. Политика описывает условия и результат обработки событий. Событие фиксирует наблюдение, инцидент выделяет его для расследования, а действие изменяет состояние компьютера только после исполнения. Включение канала само по себе не создаёт инцидент.

Атрибуты политики

Политика объединяет правила одного канала и задаёт, для каких клиентов и пользователей они действуют. Настройки функций агента задаются отдельно в разделе возможностей.

Поле / атрибут	Значение и влияние
Название	Название в каталоге, карточках и связанных событиях. Помогает определить назначение политики; само по себе не является условием срабатывания.
Описание	Пояснение цели и области контроля для администратора. Не участвует в сопоставлении события и не задаёт действие на компьютере.
Политика включена	Включает оценку правил этой политики на подходящих клиентах. Выключенная политика остаётся в каталоге, но её правила не участвуют в принятии новых решений. Отключение не отменяет уже выполненные действия.

Поле / атрибут	Значение и влияние
Канал	Определяет источник событий, набор доступных условий и допустимых действий. В одной политике используется один канал. Контроль USB-накопителей и остальных USB-устройств настраивается раздельно.
Приоритет политики	Число, определяющее порядок обработки совпадений между политиками: большее значение обрабатывается раньше. Сравнивается до приоритета правила. Влияет на выбор конфликтующих действий и действие исключений.
Операционные системы	Ограничивает платформы, для которых предназначена политика. В текущем редакторе доступна Windows; выбор Linux отключён.
Значок в списке / Цвет значка	Оформление записи в каталоге. Не влияет на область, условия, порядок оценки, серьёзность и действия.
Правила	Набор отдельных условий и реакций внутри политики. Каждое правило имеет собственную включённость, приоритет, режим и серьёзность. Совпасть могут несколько правил одновременно.

Область применения

Поле / атрибут	Значение и влияние
Ко всем	Политика распространяется на подходящих клиентов рабочей области с учётом платформы и доступности канала.
К пользователям	Ограничивает применение выбранными именами пользователей, связанными с событием. Можно выбрать известные имена или добавить имя вручную. Пользователь Windows и учётная запись веб-консоли имеют разные назначения.

Поле / атрибут	Значение и влияние
К группе клиентов	Ограничивает применение компьютерами выбранных групп. Это группы клиентов в веб-консоли, а не группы пользователей Windows. Изменение состава группы меняет круг адресатов политики.
К компьютерам	Ограничивает применение выбранными клиентами. Условие относится к источнику события; отдельное правило не расширяет область своей политики.

Атрибуты правила

Поле / атрибут	Значение и влияние
Название правила	Позволяет различать совпадения внутри политики. Отображает назначение правила; название не анализируется как условие.
Правило включено	Управляет участием конкретного правила в оценке. Выключенное правило не участвует даже при включённой политике.
Приоритет правила	Определяет очередность правил после учёта приоритета политики. Более высокое значение обрабатывается раньше. В редакторе порядок меняется стрелками в списке правил; поле текущего приоритета доступно для просмотра.
Режим	Определяет результат совпадения: наблюдение, применение выбранных действий либо исключение конкретных действий. Режим не заменяет условия и не меняет область политики.
Логика условий	AND требует совпадения всех добавленных условий. OR допускает совпадение любого из них и расширяет круг срабатываний. Для установленных программ применяется AND.

Поле / атрибут	Значение и влияние
Условия	Ограничивают события по признакам выбранного канала. Если условий нет, правило относится ко всем событиям этого канала в своей области применения.
Проверять текст также в русской и английской раскладках	Для буфера обмена и клавиатуры дополнительно сопоставляет варианты раскладки захваченного текста с ключевыми словами и регулярными выражениями. Расширяет текстовый поиск; не переводит имена пользователей и пути программ.
Критичность	Уровень важности результата: низкая, средняя, высокая или критическая. Используется для отображения и оценки события или инцидента. Не увеличивает приоритет правила и не добавляет действия. При нескольких совпадениях учитывается наиболее высокий уровень.
Действия на компьютере	Операции, которые требуется выполнить при совпадении в режиме применения действий. Доступный список зависит от канала. Назначение действия не гарантирует его успешного выполнения Windows.
Исключаемые действия	Список конкретных операций, отменяемых правилом-исключением для совпавших событий с учётом приоритетов. Не является общим разрешением всего канала.
Реакции	Создание инцидента и уведомление пользователя. Это отдельные последствия совпадения; они не заменяют выбранные действия на компьютере.

Режимы правила

Режим	Результат
Наблюдение	Совпадение фиксируется без действий на компьютере; создание инцидента и уведомление пользователя задаются отдельно.
Применить действия	Нужно явно выбрать хотя бы одно поддерживаемое действие. Само решение deny не означает универсальную блокировку.
Исключение	Укажите конкретные действия, которые исключаются для совпадения. Исключение не отключает весь агент и все остальные каналы.

Приоритеты и несколько совпадений

Движок рассматривает включённые применимые правила, включая несколько совпадений. Сначала сравнивается приоритет политики, затем правила, от большего к меньшему. Более приоритетное исключение подавляет указанные действия нижестоящих совпадений. Совместимые действия могут объединяться; для конфликтующих действий одной категории выбирается более приоритетное. При равных приоритетах не рассчитывайте на порядок отображения: задайте разные значения и проверьте итоговый план.

Правило может совпасть, но его действие будет подавлено исключением или конфликтом. Если разрешающее правило подавило все действия нижестоящего запрета, этот запрет не должен создавать инцидент и уведомление. Если конфликтующим действием победило другое правило, реакции совпавшего правила могут сохраниться. Поэтому проверяйте совпавшие правила, подавленные действия и фактические результаты отдельно.

Редакторы каналов

Канал	Обозначение	Назначение и условия	Действия и ограничения
Буфер обмена	clipboard	Проверка текста буфера в контексте процесса и окна; обнаружение чувствительных фрагментов.	Очистка или замена текста, реакции на процесс и сессию. Не гарантирует отмену уже выполненной передачи.

Канал	Обозначение	Назначение и условия	Действия и ограничения
Клавиатура	keyboard	Проверка вводимых последовательностей и контекста окна для выявления запрещённого ввода.	Реакции на процесс и сессию. Наличие наблюдения не означает перехвата всех способов ввода.
Приложения	applications	Контроль процессов, исполняемых файлов, окон и признаков программ удалённого доступа.	Закрытие приложения, завершение процесса или дерева. Для принудительного завершения нужны имя процесса либо путь EXE; одного заголовка окна недостаточно.
USB-накопители	usb	Контроль подключений и свойств съёмных дисков; применение режима доступа.	Отключение, запрос извлечения, только чтение. Занятость диска и поддержка Windows влияют на результат.
USB-устройства	usb_devices	Контроль USB-функций по типу и идентификаторам, включая устройства вне категории накопителей.	Запрет либо ожидание подтверждения администратора. Хабы и контроллеры исключены; доступ накопителей управляется отдельно.

Канал	Обозначение	Назначение и условия	Действия и ограничения
Установленные программы	installed_programs	Контроль наличия и изменений состава ПО, издателя и версии.	Требование исправления с текстом и сроком. Автоматическая установка/деинсталляция и проверка отсутствующего обязательного ПО не поддерживаются текущим редактором.
Сетевые интерфейсы	network_interfaces	Контроль Wi-Fi, Ethernet, VPN и виртуальных адаптеров по их свойствам и состоянию.	Отключение адаптера, отключение Wi-Fi или изоляция компьютера. Это не анализ содержимого всего сетевого трафика.
Telegram	telegram_content	Переписка, отправка, вложения и контекст чата.	Задержка отправки, действия с полем и сообщениями, фиксация материалов; зависит от данных агента.
Скриншоты	screenshots	Попытки снимка по сочетанию клавиш или программе захвата.	Запрет снимка и фиксация материалов; Win+PrintScreen может обрабатываться удалением файла после создания.
Сертификаты Windows	certificates	Хранилище, отпечаток, цепочка, субъект, назначение и срок.	Наблюдение, удаление совпавшего сертификата, блокировка экрана или изоляция сети.

Канал	Обозначение	Назначение и условия	Действия и ограничения
Безопасность Windows	os_security	Тестовая подпись, целостность ядра, отладка, BCD и Secure Boot.	Наблюдение, исправление BCD с перезагрузкой, блокировка экрана или изоляция сети.

Как сопоставляются значения условий

Состав сохранённых сведений зависит от канала и настроек хранения. Отсутствие фрагмента текста не доказывает отсутствие совпадения; изменение заголовка окна может вызвать повторную оценку.

Несколько значений одного списка задают альтернативы: достаточно совпадения одного значения. Ввод списков разделяется запятыми или переносами строк. Пустое поле не добавляет ограничение. AND/OR связывает добавленные условия, а не отдельные элементы списка. Ключевые слова и регулярные выражения содержимого проверяются совместно: совпадения одного из них достаточно для текстового условия; то же относится к словам и выражениям текста окна.

Текстовые списки обычно ищут вхождение без учёта регистра. Поле «Имя процесса» сравнивает полное имя исполняемого файла, а «Полный путь EXE» - полный нормализованный путь. Серийные номера и PNP ID сравниваются как идентификаторы, а не как произвольные части текста. Регулярные выражения задают шаблон поиска; некорректное выражение не даёт совпадения. Недоступное текстовое содержимое окна не подтверждает совпадение условия по его тексту.

Условия: буфер обмена

Поле / атрибут	Значение и влияние
Состояние буфера	Доступно изменение содержимого. Привязывает правило к обновлению буфера; не означает полноценное отслеживание каждой вставки в приложение.
Процесс-источник	Список имён процессов, связанных с источником содержимого. Используется текстовое сопоставление без учёта регистра; относится к источнику, а не к программе назначения.

Поле / атрибут	Значение и влияние
Тип данных	Текст или файл. Ограничивает содержимое по его виду; список из обоих вариантов допускает любой из них.
Расширения файлов	Список расширений. Ограничивает файловое содержимое по окончанию имени файла. Не анализирует внутренний формат и не подтверждает его соответствие расширению.
Слова в содержимом	Список слов или фраз для поиска в доступном содержимом. Совпадение допускается как часть текста, без учёта регистра.
Регулярные выражения	Список шаблонов поиска в содержимом. Позволяет описать структуру текста вместо перечисления отдельных слов.

Условия: клавиатура

Поле / атрибут	Значение и влияние
Паттерн ввода	Доступен признак быстрой равномерной серии разных клавиш. Выбирает события, для которых агент распознал такой характер ввода; сам по себе не устанавливает происхождение ввода.
Процессы	Текстовый список процессов, связанных с вводом. Сужает правило по контексту источника события.
Активный процесс	Список точных имён исполняемых файлов активного приложения. Отделяет ввод в выбранных приложениях от остального ввода.
Заголовок окна	Слова или фразы в заголовке активного окна. Ограничивает контекст ввода; не равнозначно поиску текста внутри окна.
Набранный текст: ключевые слова	Ищет слова и фразы в доступном набранном тексте. Учитывает настройку проверки раскладок.

Поле / атрибут	Значение и влияние
Набранный текст: регулярные выражения	Ищет заданные шаблоны в доступном набранном тексте. Работает с собранным содержимым, а не с будущим вводом.

Условия: USB-накопители

Поле / атрибут	Значение и влияние
Операция	Подключение, уже подключённый накопитель при обновлении политики или отключение. Подключение и повторная оценка при обновлении политики - разные основания срабатывания; выбираются отдельно.
Серийные номера	Список точных идентификаторов накопителя, доступных агенту. Ограничивает правило конкретными носителями; не является признаком разрешённости без соответствующего режима правила.
PNP ID накопителей	Список идентификаторов устройств Windows. Уточняет аппаратный объект, к которому относится событие. Название поля не делает его автоматически белым списком.
Тип устройства	Список типов носителя, переданных агентом. Ограничивает круг накопителей по классификации.
Файловая система	Список файловых систем тома. Ограничивает совпадение по доступным сведениям о файловой системе; не проверяет содержимое файлов.

Условия: USB-устройства

Поле / атрибут	Значение и влияние
Доверие к устройству	Недоверенное, доверенное или однократно одобренное. Выбирает состояние допуска USB-функции. Устройства исходного слепка сохраняют доверие при переподключении; однократное одобрение отличается от постоянного доверия.
Тип USB-функции	Клавиатура, мышь, камера, аудио, сеть, принтер или другой тип. Определяет контролируемую функцию. USB-накопители относятся к отдельному каналу.
Идентификаторы устройств	Список точных PNP-идентификаторов контролируемых USB-функций. У составного устройства отдельные функции могут иметь разные идентификаторы.
Событие	Подключение либо оценка уже подключённого устройства при обновлении политики. Позволяет отдельно охватить новые подключения и имеющиеся устройства.

Условия: приложения

Поле / атрибут	Значение и влияние
Событие	Запуск или закрытие приложения, изменение окна, скрытие окна, обнаружение защищённого окна либо окно удалённой сессии. Определяет основание оценки; защита окна от захвата и его скрытие - разные признаки.
Имя процесса	Список точных имён исполняемых файлов. Указывает целевой процесс. Для принудительного завершения процесса или его дерева необходим этот признак либо полный путь EXE; одного заголовка окна недостаточно.

Поле / атрибут	Значение и влияние
Полный путь EXE	Список полных путей исполняемых файлов. Различает программы с одинаковым именем. Сопоставление не учитывает регистр и нормализует разделители пути.
Заголовок окна	Слова или фразы в заголовке. Позволяет ограничить правило по названию окна; не устанавливает подлинность приложения.
Текст окна: ключевые слова	Слова и фразы в доступном текстовом содержимом окна. Возможность совпадения зависит от получения этого содержимого агентом.
Текст окна: регулярные выражения	Шаблоны поиска в доступном тексте окна. Не используются вместо заголовка и не обеспечивают чтение недоступного содержимого.
Класс окна	Текстовые признаки класса окна Windows. Уточняет тип окна; не заменяет идентификацию процесса.
Состояние окна или процесса	В фокусе, видимо, свёрнуто, скрыто или фоновый процесс. Выбирает положение окна либо отсутствие обычного видимого окна у процесса.
Удалённый доступ	Список признаков средств удалённого доступа в контексте процесса или окна. Ограничивает правило распознанными признаками; не является анализом сетевого трафика.
Защищённое окно	При включении требует признак защиты окна от захвата средствами Windows. Это отдельное условие, а не действие по включению защиты.
Скрытое окно	При включении требует, чтобы окно не было видимым. Снятый флажок не означает обязательное наличие видимого окна: ограничение просто не добавляется.

Поле / атрибут	Значение и влияние
Окно удалённой сессии	При включении требует соответствующий признак удалённого контекста окна. Не включает и не отключает удалённое подключение.

Условия: установленные программы

Поле / атрибут	Значение и влияние
Тип контроля	«Запрещённая программа» обозначает нежелательное ПО, «Положительное срабатывание» - регистрацию наличия выбранного ПО. Положительный контроль использует режим исключения и требует название или издателя; не обозначает проверку отсутствия обязательной программы.
Название	Список слов или фраз в названии из инвентаризации установленного ПО. Сопоставляется без учёта регистра. Не относится к имени запущенного процесса.
Издатель	Список слов или фраз в сведениях об издателе установленной программы. Это атрибут инвентаризации, а не самостоятельная проверка цифровой подписи.
Версия	Список текстовых значений версии. Используется поиск вхождения; поле не задаёт числовой диапазон версий и не сравнивает, какая версия новее.
Изменение	Наличие, добавление, удаление или изменение записи ПО. Для доступных типов запрещённого и положительного контроля допускаются наличие, добавление и изменение; удаление не подходит для сохранения такого правила. Проверка отсутствия ПО не поддерживается.

Поле / атрибут	Значение и влияние
Логика условий	Всегда AND: признаки названия, издателя, версии и события совместно сужают круг совпадений. Наличие ПО не доказывает, что оно запущено или используется.

Условия: сетевые интерфейсы

Этот канал контролирует конфигурацию адаптеров и её изменения. Поля редактора не задают фильтрацию сайтов, портов и содержимого сетевых пакетов.

Поле / атрибут	Значение и влияние
Изменение сети	Любое изменение, добавление или удаление интерфейса, изменение IP, DNS, шлюза, MAC, состояния либо свойств. Несколько выбранных видов являются альтернативами. «Любое изменение» относится к событиям изменения, а не к каждому снимку инвентаризации.
Тип адаптера	Wi-Fi, Ethernet, Bluetooth, VPN или виртуальный адаптер. Ограничивает событие по классификации интерфейса.
Имя интерфейса	Слова или фразы в имени, описании либо признаке типа адаптера. Используется поиск вхождения без учёта регистра; не задаёт адрес назначения соединения.
Состояние подключения	Подключён или отключён. Выбирает состояние интерфейса, известное агенту. Подключённый интерфейс сам по себе не подтверждает доступность интернета или сервера.

Новые каналы политик

Дополнение от 11 ноября 2026 года. Ниже описаны каналы и параметры текущего редактора. Они дополняют существующие правила буфера, клавиатуры, USB, приложений, установленного ПО и сетевых интерфейсов.

Условия добавляются кнопкой выбора поля. Не добавленное условие не ограничивает правило. Для добавленного логического условия установленный флажок означает «да», снятый — «нет»; чтобы вообще не проверять признак, удалите условие. Несколько значений одного списка — альтернативы; между разными условиями действует выбранная связка AND/OR.

Условия: Telegram

Контроль доступного текста, контекста чата, отправки и вложений в поддерживаемом Telegram. В редакторе канал называется «Telegram»; window_content — совместимое старое обозначение, а не отдельная новая политика. Проверяются сведения, которые передал агент: отсутствие данных о вложении или уведомлении не означает, что содержимое было полностью проверено.

Поле редактора	Значение и влияние
Направление `message_directions`	Отделяет исходящую отправку от входящего сообщения. Для запрета отправки выбирайте исходящее направление. Варианты: Исходящее (пользователь отправляет); Входящее (пользователь получает).
Тип чата `chat_types`	Ограничивает тип диалога: личный, группа, канал или бот. Варианты: Личный; Группа; Канал; Бот.
Отправитель содержит `sender_names`	Ищет указанный фрагмент в имени отправителя, переданном событием.
Отправитель: ключевые слова `sender_keywords`	Проверяет ключевые слова в имени отправителя; не является поиском по всему тексту сообщения.
Упоминания `mentions`	Проверяет признак упоминания пользователя, всех участников либо отсутствия упоминаний. Варианты: Упоминание пользователя; @all / @everyone; Без упоминаний.
Ответ на сообщение `is_reply`	Признак ответа на другое сообщение.
Пересланное сообщение `is_forwarded`	Признак пересланного сообщения.
Есть вложение `has_attachments`	Признак наличия вложения; конкретный формат уточняется условием «Тип вложения».
Пост канала `channel_post`	Отделяет публикацию канала от обычного сообщения.
Только уведомление (чат не открыт) `notification_only`	Отбор событий уведомлений, когда сам чат не открыт. Данные зависят от доступного уведомления.

Поле редактора	Значение и влияние
Чат без уведомлений (muted) `muted`	Признак отключённых уведомлений чата, если он передан источником.
Переключение из чата `from_chat_names`	Название чата, из которого произошло переключение. Используется для событий переключения.
Переключение в чат `to_chat_names`	Название чата, в который произошло переключение.
Причина переключения `switch_reasons`	Причина перехода между чатами, переданная источником. Варианты: Фокус окна; Клик; Горячая клавиша; Уведомление; Поиск.
Приложение `process_names`	Ограничивает процессы по имени EXE. Для Telegram обычно telegram.exe; для снимков — программа захвата.
Полный путь к EXE `exe_paths`	Ограничивает приложение полным путём к исполняемому файлу.
Класс окна `window_class_keywords`	Фрагменты класса окна, используемые для уточнения приложения.
Заголовок окна или чат `window_title_keywords`	Фрагменты заголовка текущего окна. Сам заголовок не подтверждает содержимое сообщения.
Название чата `chat_names`	Фрагменты названия чата. При отсутствии отдельного имени источник может передать заголовок окна.
Слова в сообщении `keywords`	Ключевые слова в доступном тексте сообщения.
Регулярные выражения `regex`	Выражения PCRE2 для текста. Регулярные выражения и ключевые слова образуют текстовое условие: достаточно совпадения одного из них.
Минимальная длина `min_chars`	Нижняя граница длины доступного текста.
Максимальная длина `max_chars`	Верхняя граница длины доступного текста.

Поле редактора	Значение и влияние
Только активное окно `foreground_only`	Ограничивает события признаком активного окна.
Тип вложения `attachment_types`	Тип вложения, определённый источником; не является проверкой всего бинарного содержимого. Варианты: Фото; Видео; Документ/архив; Аудиофайл; Голосовое; Видеосообщение; GIF; Стикер; Ссылка; Другое.
Направление вложения `attachment_directions`	Направление вложения: исходящее или входящее. Варианты: Исходящее; Входящее.
Источник обнаружения `detection_sources`	Отбор по переданному источником способу обнаружения. Выбор OCR здесь сам по себе не включает распознавание всего экрана. Варианты: Ключевое слово; Текст с фото; Ссылка; Шаблон данных; Имя или тип файла.
Домены ссылок `link_domains`	Домены ссылок, обнаруженных в сообщении; не фильтр всего сетевого трафика.

Пример: задержать отправку сообщения со словом

1. Создайте политику канала «Telegram» и выберите тестового клиента или группу.
2. Добавьте правило: направление — исходящее; процесс — telegram.exe; слова в сообщении — учебный маркер DLP_TEST. Связь условий — AND.
3. Выберите «Применить действия», затем «Задержать отправку сообщения» и «Очистить поле ввода». При необходимости включите создание инцидента.
4. Сохраните и дождитесь доставки политики. Введите учебный маркер в тестовом чате; проверьте фактическую задержку, очистку и результат действия в событии.

Блокировка, очистка и замена поля ввода требуют действия «Задержать отправку». Очистку и замену нельзя назначить одновременно. Для блокировки вложений задайте тип и направление вложения отдельно. Ctrl+Enter предусмотрен как обход задержки/блокировки ввода: такую политику нельзя описывать как безусловный запрет всех способов отправки.

Условия: Скриншоты

Контроль попыток снимка экрана по горячим клавишам и запуску известных программ захвата. Это отдельная политика, а не настройка периодического получения скриншотов в возможностях агента.

Поле редактора	Значение и влияние
Способ снимка `screenshot_methods`	Выбранные способы создания снимка. Несколько значений — альтернативы. Варианты: PrintScreen; Alt+PrintScreen (окно в буфер); Win+PrintScreen (файл в «Изображения»); Win+Shift+S (фрагмент экрана); Запуск программы захвата.
Имя процесса или программы `process_names`	Ограничивает процессы по имени EXE. Для Telegram обычно telegram.exe; для снимков — программа захвата.
Заголовок окна `window_title_keywords`	Фрагменты заголовка текущего окна. Сам заголовок не подтверждает содержимое сообщения.
Источник обнаружения `detection_sources`	Отбор по переданному источником способу обнаружения. Выбор OCR здесь сам по себе не включает распознавание всего экрана. Варианты: Горячая клавиша; Запуск программы.

Пример: ограничить снимки экрана

1. Выберите канал «Скриншоты» и нужные компьютеры.
2. Добавьте условие «Способ снимка», отметьте нужные сочетания клавиш. Для правила по программе захвата задайте соответствующее имя процесса.
3. Выберите «Применить действия → Запретить скриншот», при необходимости — создание инцидента.
4. Проверьте каждый выбранный способ на тестовом компьютере: буфер обмена, появление файла и результат действия в событии.

PrintScreen, Alt+PrintScreen и Win+Shift+S подавляются поддерживаемым перехватом. Для Win+PrintScreen на некоторых сборках Windows снимок успевает создаться: остаются удаление нового файла и очистка изображения из буфера. Известные программы захвата могут завершаться. Это не гарантия блокировки любых сторонних способов записи экрана.

Условия: Сертификаты Windows

Контроль добавления, удаления и присутствия сертификатов в хранилищах Windows. Проверка выполняется по инвентарю и событиям агента. Политика не означает автоматическое одобрение сертификата для всех браузеров и профилей.

Поле редактора	Значение и влияние
Изменение `change_types`	Отличает появление и удаление сертификата от проверки уже присутствующего. Варианты: Добавлен; Удалён; Присутствует (проверка политикой).
Хранилища `certificate_stores`	Имена хранилищ, например Root или TrustedPublisher. Уточняют место найденного сертификата.
Область `certificate_scopes`	Хранилище компьютера либо загруженного пользовательского профиля. Варианты: Компьютер; Пользователь (загруженный профиль).
Отпечатки SHA-256 или SHA-1 (точное совпадение) `certificate_thumbprints`	Точное совпадение: SHA-1 — 40, SHA-256 — 64 шестнадцатеричных символа без пробелов и разделителей.
Субъект содержит `certificate_subjects`	Фрагменты субъекта сертификата, например часть имени организации.
Издатель содержит `certificate_issuers`	Фрагменты имени издателя сертификата.
Самоподписанный (не означает угрозу; уточняйте статус цепочки) `certificate_self_signed`	Истинно для самоподписанного сертификата. Самоподписанность не означает угрозу; добавьте условия по цепочке, хранилищу или отпечатку.
Результат проверки цепочки Windows `certificate_chain_status`	Результат проверки цепочки Windows. Доверенная цепочка не равнозначна одобрению организацией; «Не проверено» не означает ни доверие, ни запрет. Варианты: Цепочка доверена Windows (не одобрение организацией); Недоверенный корень; Явно запрещён; Отозван; Недействительная подпись; Нарушен срок действия; Неполная цепочка; Ошибка цепочки; Не проверено.
Название (CN) содержит `certificate_common_names`	Фрагменты Common Name. Для однозначного исключения используйте отпечаток, а не одно название.

Поле редактора	Значение и влияние
SID профиля хранилища (точное совпадение) `certificate_user_sids`	Точный SID профиля, например S-1-5-21-…; применяется к пользовательскому хранилищу.
Серийные номера сертификатов (HEX) `certificate_serial_numbers`	Серийный номер сертификата в HEX, до 128 символов.
Назначение сертификата (OID EKU) `certificate_eku`	Назначения по OID EKU. Например, 1.3.6.1.5.5.7.3.3 — подпись кода.
Удостоверяющий центр CA (выбрано — да, снято — нет) `certificate_is_ca`	Признак сертификата удостоверяющего центра. Снятый флажок в добавленном условии означает «нет».
Просрочен (выбрано — да, снято — нет) `certificate_expired`	Признак истёкшего срока. Снятый флажок в добавленном условии означает «не просрочен».

Пример: обнаружить заданный сертификат

1. Выберите канал «Сертификаты Windows».
2. Добавьте тип изменения «Добавлен» или «Присутствует», точный SHA-256, нужное хранилище и область. Связь условий — AND.
3. Сначала задайте наблюдение и создание инцидента. Сверьте отпечаток и место обнаружения в карточке сертификата.
4. Если требуется удаление, переведите правило в применение действий и явно выберите «Удалить совпавший сертификат». Проверьте результат на целевом хранилище.

Удаляется только сертификат события из указанного хранилища; локально сохраняется его публичная копия, закрытый ключ не удаляется. Действие недопустимо для события «Удалён». Удаление может повлиять на доверие и работу приложений, поэтому широкие условия по одному CN или самоподписанности следует сначала проверить в наблюдении. Обновление справочного каталога сертификатов не выполняет это действие автоматически.

Условия: Безопасность Windows

Контроль наблюдаемых признаков работающей Windows и её загрузки: тестовая подпись, контроль целостности, отладка и Secure Boot. Отсутствие доступа к отдельной проверке отображается как неизвестное состояние и не доказывает безопасность.

Поле редактора	Значение и влияние
Проверка `change_types`	Отличает обнаруженное состояние от его изменения. Варианты: Состояние обнаружено; Состояние изменилось.
Небезопасные состояния (любое из выбранных) `os_security_flags`	Достаточно любого выбранного небезопасного состояния. Флаги работающей ОС и загрузочной конфигурации BCD проверяются отдельно; неизвестное значение не следует считать безопасным. Варианты: Тестовая подпись разрешена в работающей ОС; Контроль целостности ядра выключен; Отладка ядра включена; Отладчик ядра подключён; Отладочный режим Code Integrity; Тестовая сборка Code Integrity; Предварительная сборка Code Integrity; TESTSIGNING включён в BCD; NOINTEGRITYCHECKS включён в BCD; Отладчик загрузчика включён в BCD; Отладчик ядра включён в BCD; Secure Boot выключен.

Пример: контроль тестовой подписи Windows

1. Выберите канал «Безопасность Windows».
2. Добавьте проверку «Состояние обнаружено» и/или «Состояние изменилось», затем нужные признаки тестовой подписи работающей ОС и BCD.
3. Начните с наблюдения и инцидента. Сопоставьте событие с блоком «Безопасность Windows» в обзоре клиента.
4. Для исправления выберите «Восстановить проверку подписи и перезагрузить», задайте задержку и необходимость отключения отладки.
5. После перезагрузки проверьте повторное наблюдение и итог действия. Успешная запись параметра BCD ещё не подтверждает состояние работающей ОС.

Действие меняет текущую запись BCD, отключая тестовую подпись и отключение контроля целостности. Дополнительно может отключаться отладка. Secure Boot и установленная сборка Windows этим действием не меняются. Планируется перезагрузка, возможна потеря несохранённых данных. Повторное исправление ограничено журналом агента, чтобы не создавать цикл перезагрузок.

Шаблоны чувствительных данных в политике

В доступных текстовых каналах библиотека добавляет встроенные проверки паспорта РФ, СНИЛС, ИНН, банковских карт с Luhn, IBAN с MOD 97, API-ключей, токенов, .env, секретов конфигурации и приватных ключей. Выбор нескольких встроенных шаблонов означает совпадение с любым из них; с остальными условиями действует AND/OR правила.

1. В редакторе выберите конкретное правило и откройте Regex-библиотеку.
2. Найдите встроенный либо собственный шаблон рабочей области и примените его к выбранному правилу.
3. Проверьте добавленные условия и сочетание с другими полями, выберите наблюдение или действия.
4. Сохраните политику, проверьте поддержку агентом и испытайте её на учебных данных.

Собственные шаблоны и ручные выражения используют PCRE2. Для собственного шаблона в правило копируется выражение; правка библиотеки не обновляет сохранённую политику автоматически. Проверки контрольных сумм относятся к встроенным детекторам, а не к любому похожему regex. Для .env используются доступные имена/пути события. Шаблон не запускает сканирование диска и не превращает попытку снимка экрана в OCR содержимого. Текст, которого нет в событии, проверить невозможно.

Пример: в буфере обмена выбрать шаблон «Банковская карта · Luhn», сначала наблюдение и инцидент, затем при необходимости очистку буфера. Используйте учебный номер; совпадение контрольной суммы не означает существование действующей карты. Подробности управления библиотекой — в руководстве «Файлы, маркировки и шаблоны».

Новые действия: параметры и ограничения

Действие	Что выполняется
Задержать отправку сообщения `block_submit`	Не пропустить Enter/Submit в поле ввода до решения политики. Сообщение не уходит. Ctrl+Enter отправляет как есть.
Заблокировать вложение `block_attachment`	Не даёт отправить файл, фото, голосовое или видеосообщение. Проверка выполняется до отправки; входящее сообщение удаляется. Учитывайте направление: для входящего используется удаление через интерфейс, поэтому это не предотвращение первоначального получения.

Действие	Что выполняется
Заблокировать ввод в поле `block_input`	Не пускать новые символы и вставку в поле сообщения. Приложение остаётся активным. Ctrl+Enter снимает блокировку и отправляет.
Очистить поле ввода `clear_input`	Стереть набранный текст в поле сообщения, не отправляя его. Требуется задержка отправки; несовместимо с заменой текста в том же правиле.
Заменить текст в поле ввода `replace_input`	Подставить пояснение политики вместо набранного текста. Задайте непустой текст до 1000 символов. Требуется задержка отправки.
Удалить отправленное сообщение `delete_last_message`	Удалить последнее исходящее сообщение через интерфейс приложения. В группах ставит «Удалить для всех». Результат проверяется. При неудаче применяется выбранный откат. При неудаче выберите резервное действие: ничего, скрыть окно, запросить закрытие, завершить процесс или заблокировать экран. По умолчанию — скрыть окно. Удаление не доказывает, что получатель не успел прочитать сообщение.
Скрыть окно приложения `hide_window`	Убрать окно с экрана, не завершая процесс. Приложение продолжает работать.
Сделать скриншот `screenshot`	Снять экран сразу при срабатывании, чтобы сохранить доказательство. Используется серия кадров: сразу, через 10 и 20 секунд; частые срабатывания объединяются окном ограничения серии. Получение зависит от доступности сеанса и разрешений.
Приложить видео `video`	Приложить к инциденту доступную запись за последние 5 минут. Доступен только накопленный материал. Для вложения требуется разрешённая запись видео и хотя бы один разрешённый источник изображения: экран или камера. Звук зависит от отдельного разрешения микрофона; все источники не гарантированы.

Действие	Что выполняется
Запретить скриншот `block_screenshot`	Не даёт сделать снимок экрана: подавляет PrintScreen, Alt+PrintScreen и Win+Shift+S, завершает известные программы захвата, удаляет только что сохранённый снимок и очищает изображение из буфера обмена. Win+PrintScreen на некоторых сборках Windows обрабатывается выше пользовательского хука, поэтому для него остаётся удаление файла и очистка буфера.
Удалить совпавший сертификат `delete_certificate`	Удалить только сертификат события из указанного хранилища. Публичная копия сохраняется локально; закрытый ключ не удаляется. Выбирайте событие «Добавлен» или «Присутствует», но не «Удалён».
Восстановить проверку подписи и перезагрузить `restore_signature_enforcement`	Отключить тестовые подписи и отключение контроля целостности в текущей записи BCD. Проверить результат после перезагрузки. Secure Boot и сборка Windows не изменяются. Задержка перезагрузки — 60–3600 секунд, по умолчанию 120. Флажок отключения отладки по умолчанию выключен. Проверка результата выполняется после перезагрузки.

Для Telegram дополнительно доступны существующие действия закрытия приложения, завершения процесса/дерева, блокировки экрана, изоляции сети и отключения локальной учётной записи в поддерживаемом контексте. Для сертификатов и безопасности Windows предусмотрены также блокировка экрана и изоляция сети. Выбирайте только действия, предлагаемые редактором выбранного канала. Режим «Наблюдение» не выполняет их; исключение отменяет выбранные действия нижестоящих правил в рамках порядка применения.

Проверка новых политик после сохранения

1. Убедитесь, что выбраны нужная рабочая область, клиенты/группы и активность политики.
2. Проверьте доступность канала и требуемых возможностей у установленного агента. Старый агент может не поддерживать новое условие или действие.
3. Дождитесь подтверждения доставки. Затем отдельно проверьте совпадение правила и фактический результат действия.
4. Сопоставьте событие, инцидент, приложенные материалы и состояние целевого объекта. Отсутствие файла видео, ошибка удаления или неподтверждённая перезагрузка не считаются

успешным выполнением.

Явные действия на компьютере

Действие	Поведение и ограничения
Запросить подтверждение администратора	Отключить USB-функцию до подтверждения администратором рабочей области. Накопители управляются отдельно.
Запретить USB-устройство	Отключить USB-функцию. Разрешение требует изменения политики. Хабы и контроллеры исключены.
Отключить учётную запись и завершить сеансы	Запретить новые входы локальному пользователю события и завершить его сеансы. Несохранённые данные будут потеряны. Выполняет служба; включить учётную запись можно из управления пользователями. Администраторы, системные и доменные учётные записи защищены. Для событий без подтверждённого пользователя действие пропускается. Требуется возможность «Локальные пользователи Windows». Перед разблокировкой устраните причину срабатывания политики.
Очистить буфер обмена	Удалить содержимое, вызвавшее срабатывание.
Заменить текст в буфере	Поместить заданное сообщение вместо обнаруженного текста.
Запросить закрытие приложения	Приложение сможет предложить сохранить документ. Принудительное завершение не выполняется.
Принудительно завершить процесс	Завершить конкретный процесс, связанный с событием. Несохранённые данные могут быть потеряны.
Завершить процесс и дочерние процессы	Завершить обнаруженное дерево процессов, связанное с событием.

Действие	Поведение и ограничения
Заблокировать экран	Показать экран блокировки Windows. Пользователь разблокирует сессию самостоятельно.
Изолировать компьютер от сети	Оставить доступ только к серверу СОПКА.Рой, DNS/DHCP и loopback. Действие можно отменить из карточки клиента.
Отключить USB-накопитель	Отключить конкретное устройство средствами Windows.
Запросить извлечение накопителя	Windows может отказать в извлечении, если устройство занято.
Разрешить только чтение	Установить атрибут «Только чтение» для поддерживаемого USB-диска. Результат проверяется.
Отключить сетевой адаптер	Отключить адаптер, связанный с событием. Связь агента с сервером может прерваться.
Отключиться от Wi-Fi	Разорвать текущее Wi-Fi-подключение, сохранив адаптер включённым.
Зафиксировать требование исправить состав ПО	Добавить к событию требование и срок исправления. Установка и удаление программ автоматически не выполняются.

Параметры действий

Поле / атрибут	Значение и влияние
Текст замены буфера	Для действия замены задаётся непустой текст длиной до 1000 символов. Определяет новое содержимое буфера после успешного выполнения.
Требование по установленному ПО	Для уведомления об устранении задаётся непустой текст требования до 1000 символов и срок от 1 до 365 дней; срок по умолчанию - 7 дней. Фиксирует требование и его срок, не выполняет установку или удаление программы.

Поле / атрибут	Значение и влияние
Сочетание действий	В одном правиле допускается до 16 действий. Повтор одинакового типа не создаёт дополнительную операцию. Взаимоисключающие действия одной группы нельзя назначать вместе; редактор и проверка сохранения ограничивают сочетания.
Параметры исключения	Исключение перечисляет типы отменяемых действий. Для него не задаётся отдельный текст замены или срок требования.

Реакции и их влияние

Поле / атрибут	Значение и влияние
Запись события	Редактор сохраняет регистрацию события включённой. Даёт сведения о совпадениях и результатах. Регистрация сама по себе не блокирует операцию.
Создать инцидент	Создаёт объект для расследования при эффективном совпадении режима наблюдения или применения действий. Инцидент и действие на компьютере - самостоятельные результаты.
Уведомить пользователя	Запрашивает уведомление в поддерживаемом контексте. Для обычных каналов применяется при режиме действий; для установленного ПО предусмотрено уведомление по результату контроля. Уведомление не доказывает выполнение блокировки.
Реакции исключения	В режиме исключения редактор отключает создание инцидента и уведомление. Сохраняются регистрация и перечень исключаемых действий. Совпавшее исключение также подавляет реакции нижестоящих правил наблюдения; уже учтённые реакции более приоритетных правил оно не отменяет.

Поле / атрибут	Значение и влияние
Несколько совпадений	Реакции учитываются вместе с порядком правил и эффективными действиями. Если все действия правила отменены исключением, оно не создаёт инцидент и уведомление только на основании этих отменённых действий.
Результат выполнения	В событии различаются совпадение правила, назначенное действие и фактический результат. Ошибка Windows, недостаток прав или отсутствие целевого объекта могут помешать выполнению.

Возможности, которые не являются редакторами политик

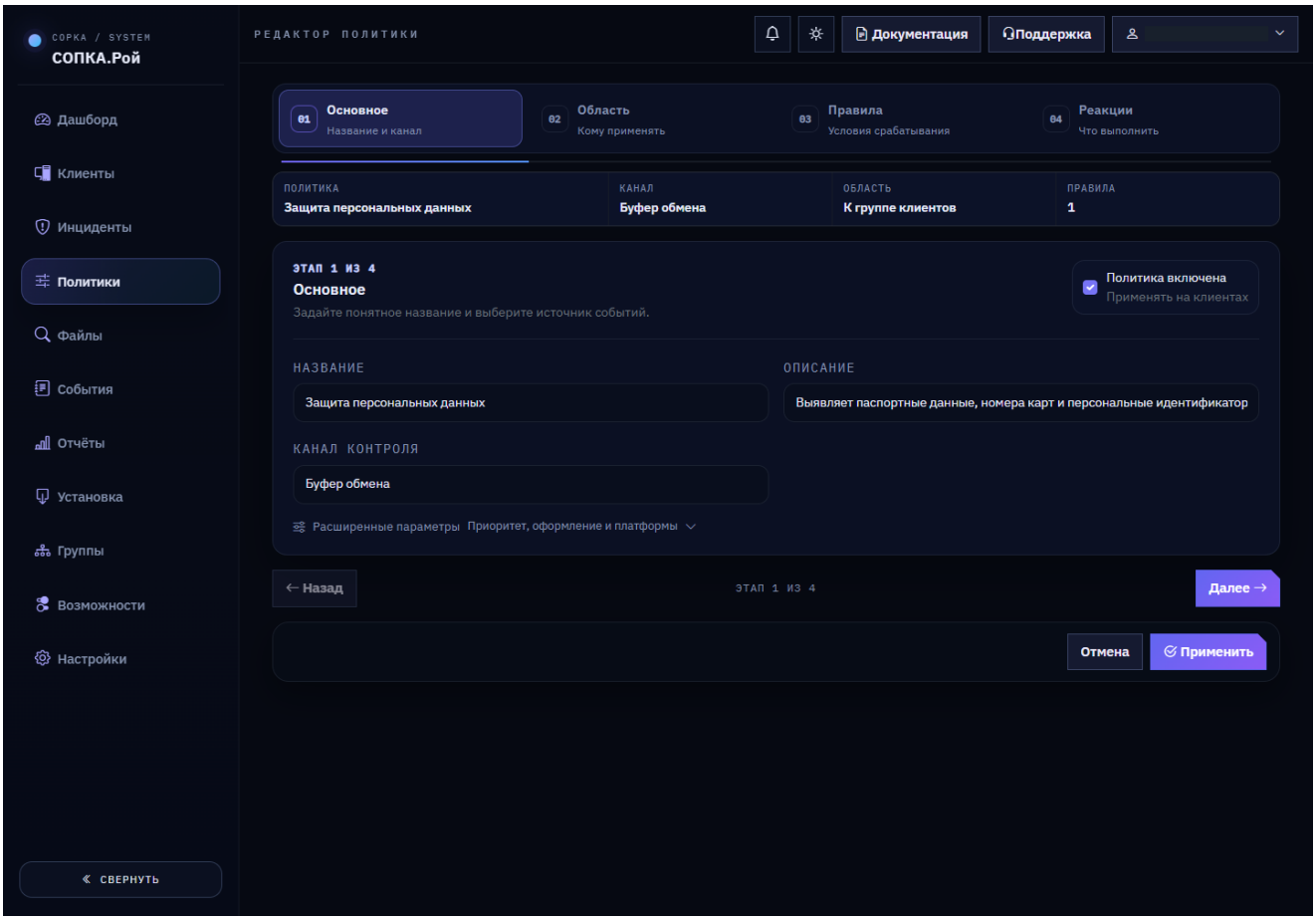
Мониторинг файлов, браузерные наблюдения, периодическое получение снимков, поиск файлов, прямой экран, удалённая консоль и карантин являются отдельными функциями. Политика «Скриншоты» отдельно контролирует попытки создания снимков; она описана выше. Наличие события такого канала не означает наличие поддерживаемой блокирующей политики. Карантин файлов выполняется отдельной файловой операцией и не входит в каталог явных действий перечисленных редакторов.

Сохранение и применение

Сохранение фиксирует настройки в консоли. Контроль начинает использовать полученную клиентом конфигурацию, если платформа, поддержка и разрешение возможностей это допускают. Изменение политики не отменяет уже выполненные действия: восстановление устройства, учётной записи или сетевого доступа выполняется отдельно.

Анализ политик в AI-чате

Редактор или администратор может запросить сводку политик и кратких правил. AI-аналитик не сохраняет редактор, не меняет приоритеты и не применяет действия. Сведения о возможностях компьютера и явные настройки группы имеют разный смысл; итог определяется наследованием и поддержкой агентом.



Подробнее: AI-чат: анализ безопасности.