ОПИСАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Функциональные характеристики

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

Назначение

СОПКА.Рой - программный комплекс класса DLP для локального или выделенного развёртывания по договору и централизованного контроля событий на рабочих станциях Windows. Сервер принимает телеметрию агентов, применяет политики, формирует инциденты и предоставляет веб-интерфейс для анализа и расследования.

Область применения

• контроль корпоративных рабочих станций, находящихся под управлением организации;

• выявление передачи чувствительных данных через контролируемые каналы;

• учёт событий приложений, файлов, буфера обмена, USB-устройств и сетевых интерфейсов;

• поиск уже существующих файлов по заданиям администратора;

• расследование инцидентов с фиксацией статуса, ответственного и комментариев;

• централизованное управление политиками и версиями Windows-агентов.

Функции версии 1.0.0

Подсистема	Возможности
Рабочие области	Изоляция клиентов, политик, событий, инцидентов, пользователей и настроек по workspace.
Агенты	Регистрация по ключу, уникальный UUID, heartbeat, получение политик, служебных команд и контроль версии протокола.
События	Приём и нормализация файловых, USB-, clipboard-, application-, network-, browser- и иных событий.
Политики	Приоритетные правила по субъекту, процессу, содержимому, устройству и сети; решения allow, deny, monitor и ignore.
Инциденты	Отдельная сущность, создаваемая по решению политики; статусы, комментарии, ответственный и история изменений.
Поиск файлов	Задания, расписания, области сканирования, метки, watchlist, карточка файла, версии, предпросмотр и контролируемая загрузка.
Экран	Ручной запрос снимка, периодические снимки по политике и прямой экран по явной команде администратора.
Уровни доступа	Роли admin, editor и viewer; приглашения в рабочую область; разграничение полномочий и изоляция данных организаций.

Правовые и организационные условия эксплуатации

СОПКА.Рой предоставляет технические функции контроля и не определяет правовое основание их применения. Эксплуатирующая организация самостоятельно определяет цели и основания обработки, перечень контролируемых каналов, категории данных, сроки хранения, локальные акты и круг уполномоченных пользователей.

- обработка должна быть законной, целевой и не избыточной по отношению к заявленным задачам;
- работники знакомятся с применимыми локальными актами и правилами использования корпоративных информационных ресурсов;

- снимки экрана, прямой экран, клавиатурные события и загрузка файлов включаются только при документированной необходимости и ограниченном ролевом доступе;
- заказчик продукта отвечает за соблюдение требований законодательства и внутренних процедур при эксплуатации системы.

Установка и сопровождение агента

Агент устанавливается по регистрационному ключу, который создаётся в рабочей области. Пакет агента не содержит название рабочей области и не хранит секрет в открытом виде внутри ZIP. После установки клиент регистрируется на сервере, получает device-токен, отправляет heartbeat и забирает подписанный bundle политик.

Поставка и развёртывание выполняются в рамках договора: состав включённых модулей, каналы контроля, сроки хранения и доступ администраторов фиксируются организационными документами заказчика.

Для сопровождения рабочих станций предусмотрен `CopkaRoyUpdater.exe`. Сервер может автоматически поставить устаревший агент в очередь обновления после heartbeat или дождаться ручной команды администратора. Пакет обновления проверяется по подписи Ed25519 и SHA-256.

Ограничения

- агент версии 1.0.0 рассчитан на Windows x64 и устанавливается с правами администратора;
- фактическое блокирование зависит от возможностей конкретного клиентского модуля; часть правил работает в режиме аудита или оповещения;
- клавиатурный контроль включается только политикой, а прямой экран запускается вручную;
- внешнее TLS-терминирование, резервное копирование и защита публичного контура настраиваются администратором;
- продукт не заявляется как сертифицированное средство защиты информации или средство криптографической защиты.