

# Краткое сравнение «Стакановец» и Falcongaze



Только для внутреннего использования

# Сравнение «Стахановец» и Falcongaze



## Функционал

	«Стахановец»	Falcongaze
Производительность	<ul style="list-style-type: none"><li>✓ Минимальная нагрузка на ЦП, подходит для слабых компьютеров, работает на Linux и Windows серверах</li></ul>	<ul style="list-style-type: none"><li>⚠ Требует более мощных серверов и выделенных ресурсов для стабильной работы с большими объёмами данных.</li></ul>
Машинное обучение и ИИ-модули	<ul style="list-style-type: none"><li>✓ Запатентованные ML-модули для прогнозирования рисков, текучести кадров и выгорания на базе ИИ-ассистента</li></ul>	<ul style="list-style-type: none"><li>⚠ Проводит ретроспективный анализ поведения (UBA) и фиксирует аномалии, но не прогнозирует кадровые риски выгорания или текучести на основе исторических данных</li></ul>
HR-аналитика и анализ поведения сотрудников	<ul style="list-style-type: none"><li>✓ Мощный многофункциональный модуль HR-аналитики: оценивает эффективность и вовлеченность сотрудников по 40+ параметров поведенческого анализа</li></ul>	<ul style="list-style-type: none"><li>✗ HR-аналитика отсутствует. Анализ поведения сотрудников только на базе отдельного модуля «Risk analysis» который строит список сотрудников с повышенным риском и выдаёт единичные отчеты по их активности</li></ul>
Антифото (защита от фотографирования экрана)	<ul style="list-style-type: none"><li>✓ Встроенная блокировка попыток фотографирования экрана мобильными устройствами</li></ul>	<ul style="list-style-type: none"><li>⚠ Только на базе отдельного модуля «Screen Photo Detector» который фиксирует съёмку через камеру, но не скрывает окно и не блокирует систему, реагируя только на встроенную веб-камеру без персонализации сценариев.</li></ul>
Биометрические возможности	<ul style="list-style-type: none"><li>✓ Клавиатурный почерк: идентификация пользователей по особенностям набора текста для предотвращения несанкционированного доступа</li><li>✓ Распознавание лиц: локальная идентификация сотрудника по образу лица с веб-камеры для предотвращения подмены учётных записей.</li></ul>	<ul style="list-style-type: none"><li>✗ Клавиатурный почерк: Отсутствует биометрия ввода, есть только перехват нажатий клавиш (Кейлоггер) без последующего анализа аномалий</li><li>⚠ Распознавание лиц: Ограниченные возможности, без локального-режима</li></ul>
Голосовое DLP	<ul style="list-style-type: none"><li>✓ Мгновенная реакция на ключевые слова при использовании микрофона в режиме реального времени</li><li>✓ Полностью локальное преобразование аудиопотока в текст без передачи на внешние серверы, гарантирующее конфиденциальность переговоров.</li><li>✓ Распознавание речи в 15+ мессенджерах при осуществлении звонков</li></ul>	<ul style="list-style-type: none"><li>✗ Отсутствует автоматическая транскрипция речи в текст. Нет встроенного онлайн-движка распознавания аудио; возможно лишь запись звука с микрофона без анализа речи и блокировки отправки</li><li>⚠ Анализирует голосовые сообщения и вызовы, выполняя распознавание речи в отчётах, но без мгновенного текстового алерта в реальном времени и без блокировок каналов связи</li></ul>

# Сравнение «Стахановец» и Falcongaze



## Функционал

Геолокация и контроль оборудования

### «Стахановец»

- **✓ Определение местоположения носимых устройств:** помогает отслеживать перемещение в чувствительных зонах где запрещено покидать периметр, а также удаленных сотрудников
- **✓ Контроль установленного оборудования:** отслеживает состояние железа и ПО на рабочих станциях и сигнализирует об их изменениях

### Falcongaze

⚠ Геолокация только по IP-адресам без комбинирования с другими источниками и без верификации подмены пользователя по геоданным, включая VPN.

Мониторинг сетевой активности

✓ Отслеживание и блокировка передачи данных по всем каналам: HTTP/S, FTP, SMTP, мессенджеры, облачные хранилища, криптоадреса; краулер по корпоративным репозиториям для поиска «запароленных» архивов.

⚠ Контроль основных каналов: POP3, SMTP, IMAP, MAPI, веб-интерфейсы, мессенджеры. Захват сетевого трафика; блокировка по правилам; нет встроенного шифрования каналов

Расширенный поиск по файлам

✓ Crawler-поиск внутри файлов, архивов и зашифрованных контейнеров с использованием регулярных выражений

✗ Не предусмотрен: SecureTower не содержит краулера по локальным файловым системам за пределами логов DLP-агента.

Цифровые отпечатки файлов и маркировка документов

- **✓ Маркирование конфиденциальных документов при помощи скрытых меток**
- **✓ Автоматическое создание цифровых отпечатков файлов и контроль изменений с возможностью гибких политик DLP**

⚠ Проводит анализ по хэшу и шаблонам, выявляя отправку документов по «цифровому отпечатку», но не поддерживает скрытые водяные знаки

Скрытые водяные знаки

✓ Нанесение скрытых и открытых «водяных знаков» на принтскрин (скриншоты) и при печати критических документов для последующей идентификации источника утечки

✗ Не маркирует скриншоты при печати

Черный ящик (Black Box запись)

✓ Непрерывная зашифрованная запись видео с экрана и аудио с микрофона для детального последующего анализа

⚠ Поддержка архивирования данных с возможностью просмотра истории активности; нет явного «чёрного ящика», отсутствует возможность полной реконструкции инцидентов

# Сравнение «Стахановец» и Falcongaze



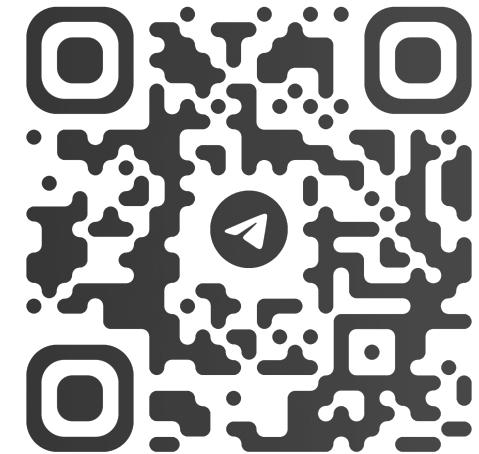
## Функционал

	«Стахановец»	Falcongaze
Мониторинг файловых операций	<ul style="list-style-type: none"><li>✓ Полный контроль копирования, переноса, удаления, буфера обмена; запрет отправки по интернету, на флэш-накопитель; DLP-политики по ключевым словам в документах (.docx, .pdf и др.) с возможностью блокировки</li></ul>	<ul style="list-style-type: none"><li>⚠️ Базовый аудит файловых операций с использованием контрольных сумм, без контент-анализа (текущие папки, теневое копирование); блокировка USB-устройств. Высокая нагрузка при расширенном мониторинге из-за постоянного сбора данных</li></ul>
Веб-активность и URL-мониторинг	<ul style="list-style-type: none"><li>✓ Контроль посещённых сайтов с оценкой «полезности» действий; уведомления о нежелательных ресурсах; гибкие политики блокировки</li></ul>	<ul style="list-style-type: none"><li>⚠️ Есть базовая фильтрация URL и логирование посещений, но отсутствует полноценный мониторинг веб-активности и автоматическая блокировка нежелательных ресурсов</li></ul>
Веб-интерфейс	<ul style="list-style-type: none"><li>✓ Интуитивный веб-GUI интерфейс с гибкой настройкой прав доступа</li></ul>	<ul style="list-style-type: none"><li>⚠️ Многоуровневый интерфейс с разделением функций по модулям, требует обучения, менее гибкий в настройке и менее дружественный для быстрого реагирования ИБ специалистов на инциденты</li></ul>
Граф связей	<ul style="list-style-type: none"><li>✓ Визуализирует «граф связей» сотрудников на основе всех каналов коммуникации и активности, позволяя выявлять аномальные паттерны взаимодействия и рисковые группы.</li></ul>	<ul style="list-style-type: none"><li>⚠️ Устанавливает привязку каналов связи (email, IM, IP) к карточкам пользователей в AD, но не строит интерактивный социальный граф для анализа коммуникаций.</li></ul>
Работа в терминальном сервере	<ul style="list-style-type: none"><li>✓ Тонкий клиент, вся обработка данных ведется на сервере; полноценный контроль многопользовательских сессий без дополнительной настройки, тонкие клиенты не нагружают сеть, ЦП, RAM и не требуют локальной установки субагентов.</li></ul>	<ul style="list-style-type: none"><li>⚠️ SecureTower мониторит терминальные сессии через агент на сервере, собирая логи и скриншоты, однако не разграничивает визуально пользователи на RDP/ICA, что затрудняет детальный анализ отдельных сессий</li></ul>
Удалённое администрирование	<ul style="list-style-type: none"><li>✓ Экстренная блокировка клавиатуры/мыши, администрирование политик и прав онлайн без остановки агентов.</li></ul>	<ul style="list-style-type: none"><li>⚠️ Поддерживается через автоматический запуск пользовательских скриптов при срабатывании правил безопасности, позволяющий заблокировать рабочую станцию; требует дополнительной конфигурации и навыков написания скриптов</li></ul>
Уникальный функционал	<ul style="list-style-type: none"><li>✓ ИИ-ассистент, Антифото, клавиатурный почерк, Black Box, голосовое DLP, антимайнинг (CPU/GPU)</li></ul>	<ul style="list-style-type: none"><li>⚠️ Распознавание штампов (stamps recognition) для контроля подлинности документов, перехват и анализ файлов САПР (CAD-software files)</li></ul>

↗ [stakhanovets.ru](http://stakhanovets.ru)

↗ +7 (499) 110-64-10

↗ [partners@stakhanovets.ru](mailto:partners@stakhanovets.ru)



@STAKHANOVETS\_RU

Наш Телеграм - канал, где все  
актуальные новости по ИБ, ЕМ и DLP