

Краткое сравнение «Стахановец» и Zecurion

Только для внутреннего использования

stakhanovets.ru



Сравнение «Стахановец» и Zecurion



Функционал	«Стахановец»	Zecurion
Производительность	✓ Минимальная нагрузка на ЦП, подходит для слабых компьютеров, работает на Linux и Windows серверах	⚠ Агент постоянно шлёт метаданные и контент на сервер; нагрузка на сеть и СУБД растёт линейно с числом клиентов; для крупных нагрузок требуется кластерная инфраструктура и терминаторы SSL; нагрузка может создавать очереди
Машинное обучение и ИИ-модули	✓ Запатентованные ML-модули для прогнозирования рисков, текучести кадров и выгорания на базе ИИ-ассистента	⚠ Выявление аномалий только по статическим правилам без предиктивных функций; отсутствие биометрических ИИ-модулей и offline-обработки данных; традиционный подход к анализу без современных нейросетевых алгоритмов и машинного обучения
Кадровая аналитика и учет рабочего времени	✓ Мощный многофункциональный модуль HR-аналитики: оценивает эффективность и вовлеченность сотрудников по 40+ параметров поведенческого анализа	⚠ Staff Control: отдельный модуль ведет логи действий, время работы и эффективность на основе 10+ индикаторов, но без полноценного табеля прихода/ухода и унифицированных HR-отчётов
Антифото (защита от фотографирования экрана)	✓ Встроенная блокировка попыток фотографирования экрана мобильными устройствами	⚠ Отдельный модуль Screen Photo Detector реагирует на попытки съемки через веб-камеру, но не скрывает окно приложения и не блокирует всю систему; распознаёт только встроенную камеру, без персонализации сценариев блокировки.
Биометрические возможности	<ul style="list-style-type: none">✓ Клавиатурный почерк: идентификация пользователей по особенностям набора текста для предотвращения несанкционированного доступа✓ Распознавание лиц: локальная идентификация сотрудника по образу лица с веб-камеры для предотвращения подмены учётных записей.	<ul style="list-style-type: none">✗ Клавиатурный почерк: Отсутствуют встроенные модули для биометрического анализа клавиатурного почерка.✗ Распознавание лиц: Нет встроенного оффлайн-распознавания лиц; идентификация через учетные записи и атрибуты AD без биометрии
Голосовое DLP	<ul style="list-style-type: none">✓ Мгновенная реакция на ключевые слова при использовании микрофона в режиме реального времени✓ Полностью локальное преобразование аудиопотока в текст без передачи на внешние серверы, гарантирующее конфиденциальность переговоров.✓ Распознавание речи в 15+ мессенджерах при осуществлении звонков	<ul style="list-style-type: none">⚠ Нет штатного модуля для непрерывного голосового мониторинга; возможна запись аудио в рамках Device Control, но без ASR-реакции в реальном времени и без локального оффлайн-STT



Сравнение «Стахановец» и Zecurion



Функционал

«Стахановец»


Zecurion


Геолокация и контроль оборудования

-  **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


-  **Определение местоположения носимых устройств:** нет встроенной функции геолокации; отсутствует контроль координат рабочих мест.
-  **Контроль установленного оборудования:** Device Control Agent фиксирует только подключение/отключение внешних устройств (USB, принтеры) без полноценной инвентаризации и централизованных отчетов и отслеживания изменений в конфигурации ПК


Мониторинг сетевой активности

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



-  Мониторинг и контроль трафика более 100 каналов (SMTP, POP3, IMAP, HTTP(S), FTP, мессенджеры, облачные сервисы) через активный фильтр или SPAN-зеркалирование; SSL-дешифрование MITM-подходом для анализа HTTPS; базовая фильтрация по словарям и шаблонам


Расширенный поиск по файлам

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


-  Ограниченный краулер, поддерживающий обход только локальных сетевых хранилищ и SharePoint, без OCR и семантического анализа; работает по расписанию, без real-time обхода и автоматической классификации, результаты требуют ручной обработки.


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


-  Поиск по цифровым отпечаткам текста и графики с возможностью обнаруживать совпадения фрагментов; нет механизма авто-обновления отпечатков и отсутствует инструмент маркировки файлов.


Скрытые водяные знаки

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

-  Отображение видимых водяных знаков (имя пользователя, ПК, дата) поверх окон приложений; нет поддержки невидимых или цифровых скрытых водяных знаков.

Черный ящик (Black Box запись)

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

-  Нет поддержки полноценной видео/аудио «черного ящика»; ведется только событийный лог действий пользователя (файловые операции, нажатия клавиш, сетевые сессии) без видео-аудио контекста.

Сравнение «Стахановец» и Zecurion

Функционал

«Стахановец»

Zecurion

Мониторинг файловых операций

✓ 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

⚠ Фиксирует базовые операции с файлами (чтение, запись, удаление) на уровне файловой системы, записывает атрибуты файлов и действия пользователей, но не выполняет глубокий контекстный анализ содержимого «на лету» и не использует ML-модели для классификации операций

Веб-активность и URL-мониторинг

✓ Контроль посещённых сайтов с оценкой «полезности» действий; уведомления о нежелательных ресурсах; гибкие политики блокировки

⚠ Применяет политики URL-блокировок по доменам, параметры запросов не анализируются глубоко, поддерживает карантин электронной почты, интеграцию с отдельным Secure Web Gateway для расширенной категоризации и фильтрации веб-ресурсов

Веб-интерфейс

✓ Интуитивный веб-GUI интерфейс с гибкой настройкой прав доступа

✓ Единая веб-консоль для всех модулей и централизованного управления: настройка политик и просмотр отчетов через один интерфейс; настраиваемая панель управления с виджетами; адаптивный дизайн для десктопа и планшета

Граф связей

✓ Визуализирует «граф связей» сотрудников на основе всех каналов коммуникации и активности, позволяя выявлять аномальные паттерны взаимодействия и рискованные группы.

⚠ Статические схемы связей на основе логов событий; модуль Staff Control выводит «карты активности», но без интерактивных фильтров и предиктивного анализа; ручная подготовка данных.

Работа в терминальном сервере

✓ 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.

⚠ Агент на каждом сеансе: требует установки отдельного агента на каждый виртуальный десктоп или сессию; повышенная нагрузка на сервер при большом числе подключений; сложное централизованное управление.

Удалённое администрирование

✓ Экстренная блокировка клавиатуры/мыши, администрирование политик и прав онлайн без остановки агентов.

⚠ Ограниченное «блокирование» через Device Control – запрет доступа к периферии (USB, Wi-Fi и др.), но нет штатного механизма мгновенной блокировки входа или мыши/клавиатуры на станции пользователя

Уникальный функционал

✓ ИИ-ассистент, Антифото, клавиатурный почерк, Black Box, голосовое DLP, антимайнинг (CPU/GPU)

⚠ Discovery Agent: корпусный поиск по базе данных и облаку с 10 технологиями детекции. Incident Workflow Automation для автоматизации расследований

➤ stakhanovets.ru

➤ +7 (499) 110-64-10

➤ partners@stakhanovets.ru



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