Стахановец

внедрение в крупный бизнес и МСП

Стахановец

Создан командой опытных управленцев, профессионалов в разработке систем контроля эффективности персонала и защиты информации

16 лет
на ИТ-рынке России с 2009 года

20 000
внедрений в РФ и других странах

10 версия
программного продукта

Российский продукт
Внесен в Единый реестр российского ПО МинЦифры

Патенты РФ
Разработки «Стахановец» запатентованы в РФ

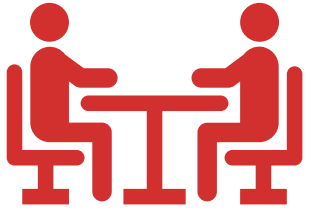
Лицензия ФСТЭК
На деятельность по разработке и производству средств СЗИ

Наша целевая аудитория — представители компаний-заказчиков

Стахановец

- Службы Безопасности (ИБ, КБ)
- Отделы по борьбе с экономическими преступлениями (ОБЭП)
- Отделы информационных технологий (ОИТ)

- C-level и топ-менеджмент
- Менеджеры среднего звена
- Руководители 1-го уровня



- Директора по персоналу (HRD)
- HR бизнес-партнеры
- HR People Partner
- Кадровые делопроизводители

Какие проблемы бизнеса решает комплекс Стахановец?

Стахановец

- Обеспечение собственной безопасности бизнеса
- Снижение финансовых и репутационных рисков
- Снижение рисков разглашения персональных данных
- Выявление промышленного шпионажа
- Выявление коррупционных схем и сговоров, сбор доказательной базы
- Рост дохода, оптимизация расходов и интенсификация усилий

Три версии комплекса

Стахановец

₽ ₽

Полный контроль — DLP-система для предотвращения утечек данных, выявления внутренних нарушителей и проведения расследований

- Контроль утечек данных
- Анализатор рисков
- Контроль файловых операций
- Уведомления об инцидентах

₽ ₽ ₽

ПРО — DLP-система и комплекс для кадрового анализа.
Содержит все функции Полного Контро
и Квант, а также дополнительные опции

- Антифото
- Маркировка документов
- Расчет уровня рисков сотрудников
- Краулер

₽

Квант — комплекс для анализа рабочей активности и проведения кадрового анализа

- Интеллектуальная система аналитики
- Анализатор производительности
- Учет рабочего времени
- Снимки экранов

Повышение эффективности персонала и DLP

Стахановец

- голосовое DLP: контроль аудиокоммуникаций
- анализатор рисков и сводный отчет
- файловые операции: контроль, перехват, запрет
- каналы перехвата: e-mail и 25 мессенджеров
- поиск по файлам на клиентской машине
- СУРВ и мониторинг АРМ
- физическая безопасность: антифото
- геолокация: определение местонахождения ноутбуков
- КРИПТОбезопасность: перехват и проверка адресов кошельков

Система кадровой аналитики и профилирования персонала

Стахановец

- профайлинг сотрудников по заданным метрикам
- интерактивные дашборды и инфографика с данными
- поиск демотивированных сотрудников
- управление эффективностью
- сравнение данных по сотрудникам и отделам
- поведение сотрудников за разные периоды
- контроль и оценка вовлеченности
- выявление лидеров по заданным метрикам

Наши основные преимущества

Стахановец

- низкие системные требования к серверной части и АРМ
- простое внедрение и обслуживание
- совместимость с антивирусным ПО
- масштабируемость на 35 000+ АРМ
- оперативная техподдержка

Enterprise-сегмент: боли клиента

Стахановец

Enterprise-сегмент включает в себя крупные корпорации с численностью персонала от 1000 до нескольких десятков тысяч сотрудников, часто имеющие территориально распределенную структуру с множественными офисами и подразделениями.

Технически-организационные проблемы

- **Проблема интеграции с существующей инфраструктурой:** 35% компаний сталкиваются с серьезными сложностями внедрения DLP-системы в существующую корпоративную инфраструктуру.
- **Недооценка необходимых ресурсов:** Как инфраструктурных, так и кадровых для реализации внедрения.
- **Высокие требования к серверному оборудованию:** Некоторые DLP-системы требуют значительно больше серверных ресурсов, что может увеличить стоимость проекта на 20-40%.

Функциональные разочарования

- **Несоответствие заявленного функционала реальности:** 65% компаний жалуются на отсутствие или некорректную работу заявленной функциональности.
- **Недостаток необходимого функционала:** 53% организаций отмечают нехватку функциональности для решения своих специфических задач.

Потребность клиента

Стахановец

Необходимость DLP-систем: КРИТИЧЕСКИ НЕОБХОДИМО

- **Высокая стоимость утечки:** Потенциальный финансовый и репутационный ущерб от утечки данных в корпорации может достигать сотен миллионов рублей.
- **Сложные регуляторные требования:** Обязательное соблюдение российских и международных и отраслевых стандартов (152-ФЗ, 420-ФЗ, GDPR, HIPAA, PCI DSS и др.), которые прямо требуют контроля за конфиденциальными данными.
- **Ценность интеллектуальной собственности:** Защита коммерческой тайны, патентов, стратегических планов и R&D является ключевым фактором конкурентоспособности.
- **Масштаб и сложность инфраструктуры:** Огромное количество сотрудников, устройств и каналов коммуникации невозможно контролировать вручную, что делает автоматизированные DLP-системы единственным решением.
- **Высокий риск инсайдерских угроз:** В больших коллективах сложнее отследить нелояльных сотрудников или случайные ошибки, которые могут привести к утечкам.

Необходимость HR-аналитики и мониторинга: КРИТИЧЕСКИ ВАЖНО

- **Масштаб персонала требует системного подхода:** В крупных корпорациях управление персоналом без аналитики становится практически невозможным.
- **Комплексные аналитические потребности:** Необходимость глубокого анализа поведенческих паттернов сотрудников для выявления инсайдерских угроз.
- **Регулятивные требования:** Многие отраслевые регулятивы требуют детального мониторинга и отчетности по персоналу.
- **Интеграция с DLP-системами:** Возможность создания комплексного профиля сотрудника для поведенческого анализа и превентивного выявления угроз.

Требования клиента

Стахановец

Технические требования и сложность

- Необходимость поддержки высокоскоростной обработки больших объемов данных
- Способность работать с территориально распределенной сетью предприятия
- Возможность масштабирования без потери производительности
- Интеграция с существующей сложной IT-инфраструктурой
- Поддержка множественных протоколов, каналов связи и устройств

Функциональные потребности

- Комплексная защита всех возможных каналов утечки информации
- Создание защищенного периметра по всем каналам передачи данных
- Единый центр управления для всех подразделений
- Возможность создания общих правил и политик безопасности
- Репликация серверов и настроек между локациями

Организационные особенности

- Выделенная команда специалистов по информационной безопасности
- Сложные многоуровневые политики безопасности
- Необходимость соответствия множественным регулятивным требованиям
- Длительный цикл внедрения и настройки (до года)
- Высокие требования к документированию и аудиту

Бюджетные характеристики

- Высокий бюджет на внедрение и поддержку (от 5000000₽+ в год)
- Готовность к значительным капитальным затратам
- Инвестиции в обучение персонала и консультационные услуги
- Возможность приобретения корпоративных лицензий с большими скидками

Крупный бизнес: боли клиента

Стахановец

Крупный бизнес представляет компании с численностью от 500-1000 сотрудников, обычно имеющие региональное присутствие и развитую организационную структуру.

Проблемы планирования и ресурсов

- **Недооценка сложности внедрения:** Ожидание простоты установки при недостаточной зрелости IT-инфраструктуры.
- **Нехватка квалифицированных кадров:** Ограниченные ресурсы для обучения персонала работе с DLP-системами.
- **Необходимость в дополнительном оборудовании:** Неожиданные расходы на серверное оборудование и лицензии.

Потребность клиента

Стахановец

Необходимость DLP-систем: ВЫСОКАЯ

- **Защита репутации и бренда:** Крупные компании являются публичными и узнаваемыми, поэтому репутационные потери от утечек крайне высоки.
- **Значительные объемы данных:** Обработка большого количества клиентских, финансовых и коммерческих данных требует системной защиты.
- **Растущее внимание регуляторов:** По мере роста компания попадает под более пристальное внимание надзорных органов.
- **Структурная сложность:** Наличие нескольких офисов или подразделений усложняет ручной контроль и требует централизованных систем безопасности.
- **Конкурентная борьба:** Защита от промышленного шпионажа и увода клиентских баз уходящими сотрудниками.

Необходимость HR-аналитики и мониторинга: ВЫСОКО, ЖЕЛАТЕЛЬНО

- **Оптимизация управления растущей командой:** Компании с 500-1000 сотрудниками уже имеют достаточно данных для эффективного анализа.
- **Повышение эффективности HR-процессов:** Возможность автоматизации рутинных HR-задач и фокус на стратегических инициативах.
- **Контроль распределенной структуры:** Необходимость централизованного мониторинга нескольких офисов и подразделений.
- **Профилактика инцидентов:** ~46% специалистов признают полезность поведенческого анализа для выявления инцидентов информационной безопасности.

Требования клиента

Стахановец

Технические требования и сложность

- Средний уровень сложности инфраструктуры
- Необходимость мониторинга нескольких офисов или подразделений
- Требования к производительности выше среднего
- Интеграция с корпоративными системами управления

Функциональные потребности

- Контроль основных каналов утечки информации
- Мониторинг действий сотрудников в реальном времени
- Автоматизация процессов выявления нарушений
- Возможность централизованного управления политиками безопасности

Организационные особенности

- Наличие IT-отдела с базовыми знаниями по информационной безопасности
- Потребность в обучении персонала работе с DLP-системой
- Среднесрочный цикл внедрения (3-6 месяцев)
- Умеренные требования к соответствию регулятивным нормам

Бюджетные характеристики

- Средний уровень инвестиций (от 1000000₽+ в год)
- Поиск баланса между функциональностью и стоимостью
- Предпочтение решениям с предсказуемой стоимостью владения

Средний бизнес: боли клиента

Стахановец

Средний бизнес включает компании с численностью от 100 до 500 сотрудников, которые активно растут и развивают свою деятельность

Проблемы планирования и ресурсов

- **Нехватка IT-персонала:** Отсутствие выделенных специалистов по информационной безопасности для управления DLP.
- **Ограниченный бюджет на обучение:** Неспособность инвестировать в серьезное обучение персонала основам ИБ.
- **Проблемы с производительностью:** Особенно критично для компаний со старым парком оборудования.

Потребность клиента

Стахановец

Необходимость DLP-систем: НЕОБХОДИМО, РЕКОМЕНДУЕТСЯ

- **Растущая ценность данных:** По мере роста бизнеса накапливается критически важная информация (клиентские базы, финансовые данные, ноу-хау).
- **Повышение привлекательности для атак:** Средний бизнес часто рассматривается злоумышленниками как «легкая цель» из-за недостаточного уровня защиты по сравнению с корпорациями.
- **Риск от текучести кадров:** Сотрудники, уходя к конкурентам, могут забрать с собой ценную информацию.
- **Требования партнеров и клиентов:** Крупные заказчики и партнеры все чаще требуют от своих контрагентов наличия систем защиты данных.
- **Проактивное управление рисками:** Внедрение DLP является признаком зрелости компании и позволяет предотвратить проблемы до их возникновения, а не реагировать на последствия.

Необходимость HR-аналитики и мониторинга: УМЕРЕННО ЖЕЛАТЕЛЬНО

- **Точка роста для масштабирования:** Компании среднего размера находятся в критической точке роста, где систематизация HR-процессов становится необходимой.
- **Оптимизация ограниченных ресурсов:** Небольшие HR-команды могут значительно выиграть от автоматизации и аналитики.
- **Подготовка к росту:** Создание основы для более сложных HR-процессов при масштабировании бизнеса.

Требования клиента

Стахановец

Технические требования и сложность

- Простота установки и настройки
- Минимальные требования к IT-инфраструктуре
- Облачные решения как предпочтительный вариант развертывания
- Автоматизированная настройка базовых политик безопасности

Функциональные потребности

- Защита основных типов конфиденциальных данных
- Контроль электронной почты и файлообмена
- Мониторинг использования внешних устройств
- Базовые возможности отчетности и анализа

Организационные особенности

- Ограниченные ресурсы IT-отдела
- Потребность в быстром внедрении (1-4 недели)
- Фокус на простоте использования и управления
- Возможность использования сервисных решений на условиях аутсорсинга

Бюджетные характеристики

- Ограниченный бюджет (500000₽ в год)
- Предпочтение подписочным моделям оплаты
- Поиск экономически эффективных решений
- Чувствительность к общей стоимости владения

Стахановец

Кейс: внедрение Стахановец в «Народный банк Республики Узбекистан»

Внедрение: 1000 АРМ

Лицензии: «Стахановец: ПРО»

С помощью Стахановец руководству банка удалось:

- предотвратить нецелевой расход рабочего времени у дистанционных сотрудников
- отучить офисных специалистов от опозданий и ранних уходов, благодаря ведению учета рабочего времени
- выявить сотрудников с низким уровнем вовлечения и повысить мотивацию за счет индивидуальных программ мотивации
- сократить текучесть кадров благодаря опции по выявлению сотрудников, которые ищут работу
- предотвратить утечки данных за счет перехвата всех каналов передачи информации

Кейс: в первую неделю использования «Стахановец» выявили сотрудника, который готовил утечку конфиденциальных данных

Стахановец

«На первой неделе работы с программой:

- Предотвратили утечку, выявив сотрудника, который искал работу и готовил документы и базу контактов, чтобы забрать с собой при увольнении.
- Выявили сотрудника, который в рабочее время выполнял задания сторонней организации.
- Выявили случаи, когда сотрудники расходуют рабочее время на личное общение в мессенджерах и посещение развлекательных ресурсов».

Алдонин А.Б. Директор по безопасности «Уральского завода эластомерных уплотнений»

О компании

Уральский завод эластомерных уплотнений — ведущий производитель резинотехнических изделий для различных отраслей промышленности.

- Входит в топ-10 производителей резинотехнических изделий
- Выручка: > 1 млрд. рублей.
- 350 сотрудников

ИСПОЛЬЗУЮТ «СТАХАНОВЕЦ 10: ПРО» ДЛЯ ОФИСНЫХ СОТРУДНИКОВ

Стахановец

Кейс: неисполнение профессиональных обязанностей

Судебный прецедент

Результат: уголовное наказание в виде штрафа, подписка о невыезде

Данные о судебном иске:

Кудрина В. Н. против
ООО «Компания Полярное Сияние»

Дисциплинарное взыскание по ст. 192 ТК РФ

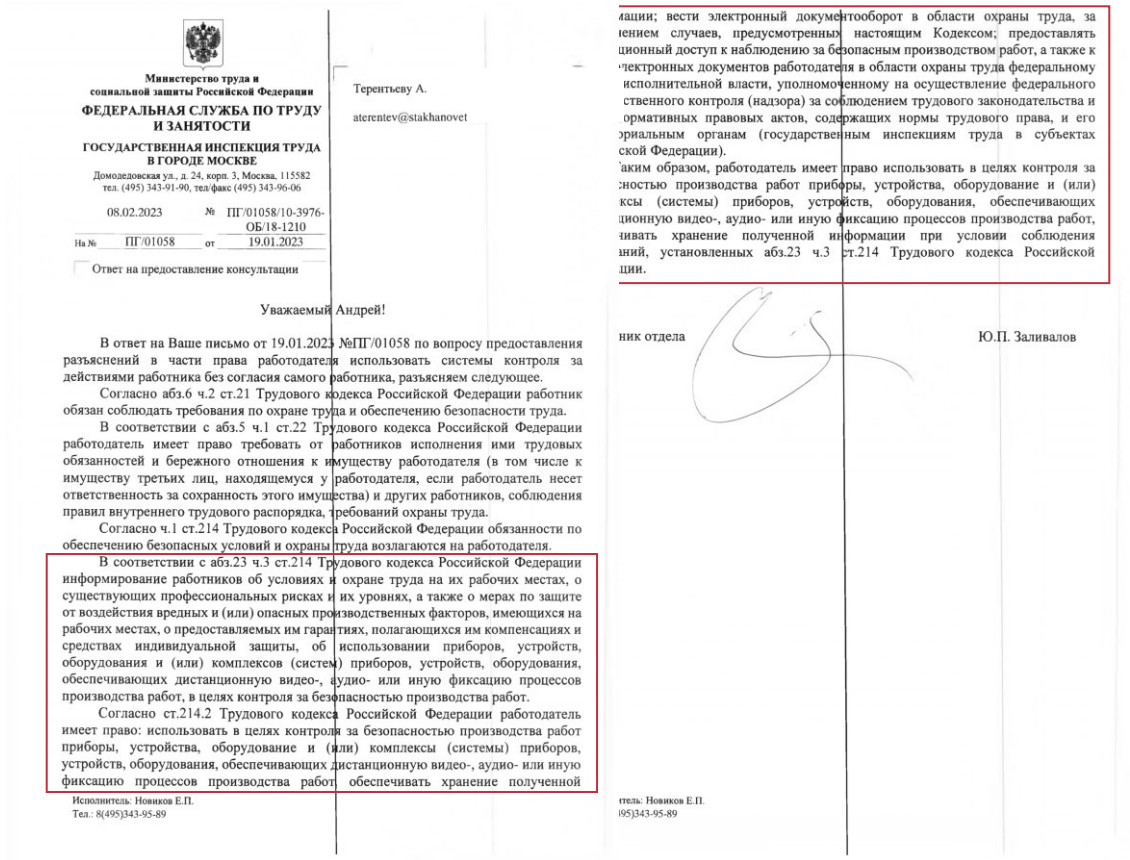
Благодаря Стахановец в компании:

- зафиксировали получение сотрудником по электронной почте задачи о необходимости выгрузки по банковским выпискам
- выявили невыполнение ежедневной рабочей обязанности в течение семи дней
- подтвердили ознакомление сотрудника с должностной инструкций и печать документа

ССЫЛКА НА МАТЕРИАЛЫ

Юридическая поддержка

Стахановец



Министерство труда и социальной защиты Российской Федерации
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТРУДУ И ЗАНЯТОСТИ
ГОСУДАРСТВЕННАЯ ИНСПЕКЦИЯ ТРУДА В ГОРОДЕ МОСКВЕ
Домодедовская ул., д. 24, корп. 3, Москва, 115582
тел. (495) 343-91-90, тел/факс (495) 343-96-06

08.02.2023 № ПГ/01058/10-3976-ОБ/18-1210
На № ПГ/01058 от 19.01.2023

Ответ на предоставление консультации

Терентьеву А.
aterentev@stakhanovet

Уважаемый Андрей!

В ответ на Ваше письмо от 19.01.2023 №ПГ/01058 по вопросу предоставления разъяснений в части права работодателя использовать системы контроля за действиями работника без согласия самого работника, разъясняем следующее.

Согласно абз.6 ч.2 ст.21 Трудового кодекса Российской Федерации работник обязан соблюдать требования по охране труда и обеспечению безопасности труда.

В соответствии с абз.5 ч.1 ст.22 Трудового кодекса Российской Федерации работодатель имеет право требовать от работников исполнения ими трудовых обязанностей и бережного отношения к имуществу работодателя (в том числе к имуществу третьих лиц, находящемуся у работодателя, если работодатель несет ответственность за сохранность этого имущества) и других работников, соблюдения правил внутреннего трудового распорядка, требований охраны труда.

Согласно ч.1 ст.214 Трудового кодекса Российской Федерации обязанности по обеспечению безопасных условий и охраны труда возлагаются на работодателя.

В соответствии с абз.23 ч.3 ст.214 Трудового кодекса Российской Федерации информирование работников об условиях и охране труда на их рабочих местах, о существующих профессиональных рисках и их уровнях, а также о мерах по защите от воздействия вредных и (или) опасных производственных факторов, имеющихся на рабочих местах, о предоставляемых им гарантиях, полагающихся им компенсациях и средствах индивидуальной защиты, об использовании приборов, устройств, оборудования и (или) комплексов (систем) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ, в целях контроля за безопасностью производства работ.

Согласно ст.214.2 Трудового кодекса Российской Федерации работодатель имеет право: использовать в целях контроля за безопасностью производства работ приборы, устройства, оборудование и (или) комплексы (системы) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ; обеспечивать хранение полученной

Исполнитель: Новиков Е.П.
Тел.: 8(495)343-95-89

...ации; вести электронный документооборот в области охраны труда, за ...ением случаев, предусмотренных настоящим Кодексом; предоставлять ...ционный доступ к наблюдению за безопасным производством работ, а также к ...лектронных документов работодателя в области охраны труда федеральному ...исполнительной власти, уполномоченному на осуществление федерального ...ственного контроля (надзора) за соблюдением трудового законодательства и ...ормативных правовых актов, содержащих нормы трудового права, и его ...риальным органам (государственным инспекциям труда в субъектах ...ской Федерации).

...аким образом, работодатель имеет право использовать в целях контроля за ...ностью производства работ приборы, устройства, оборудование и (или) ...ксы (системы) приборов, устройств, оборудования, обеспечивающих ...ционную видео-, аудио- или иную фиксацию процессов производства работ, ...ивать хранение полученной информации при условии соблюдения ...ний, установленных абз.23 ч.3 ст.214 Трудового кодекса Российской ...ции.

...ник отдела Ю.П. Заливалов

...тель: Новиков Е.П.
...95)343-95-89

- Перед внедрением любой системы мониторинга **необходимо уведомить сотрудников** о возможном наблюдении доп. соглашением к трудовому договору или пунктом в договоре. Сам комплекс может устанавливаться в открытом или закрытом режиме.

- Компания «Стахановец» предоставляет готовый пакет образцов юридических документов, необходимый Заказчикам для внедрения систем контроля и мониторинга

В соответствии с абз.23 ч.3 ст.214 Трудового кодекса Российской Федерации информирование работников об условиях и охране труда на их рабочих местах, о существующих профессиональных рисках и их уровнях, а также о мерах по защите от воздействия вредных и (или) опасных производственных факторов, имеющихся на рабочих местах, о предоставляемых им гарантиях, полагающихся им компенсациях и средствах индивидуальной защиты, об использовании приборов, устройств, оборудования и (или) комплексов (систем) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ, в целях контроля за безопасностью производства работ.

Согласно ст.214.2 Трудового кодекса Российской Федерации работодатель имеет право: использовать в целях контроля за безопасностью производства работ приборы, устройства, оборудование и (или) комплексы (системы) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ; обеспечивать хранение полученной информации; вести электронный документооборот в области охраны труда, за исключением случаев, предусмотренных настоящим Кодексом; предоставлять дистанционный доступ к наблюдению за безопасным производством работ, а также к базам электронных документов работодателя в области охраны труда федеральному органу исполнительной власти, уполномоченному на осуществление федерального государственного контроля (надзора) за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, и его территориальным органам (государственным инспекциям труда в субъектах Российской Федерации).

Таким образом, работодатель имеет право использовать в целях контроля за безопасностью производства работ приборы, устройства, оборудование и (или) комплексы (системы) приборов, устройств, оборудования, обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ, обеспечивать хранение полученной информации при условии соблюдения требований, установленных абз.23 ч.3 ст.214 Трудового кодекса Российской Федерации.

Нас выбирают

Стахановец

↗ 2 млн

АРМ под наблюдением ПО Стахановец

ЭР-ТЕЛЕКОМ

СОГАЗ

РусГидро

НЕФТЯНАЯ КОМПАНИЯ РОСНЕФТЬ

АГРОКОМПЛЕКС ВЫСЕЛКОВСКИЙ

Ростех

РОСКОСМОС

GIS ГАЗИНФОРМ СЕРВИС

НОРНИКЕЛЬ

Сравнение с конкурентами

Стахановец

Staffcop — российская система мониторинга активности сотрудников и контроля информационной безопасности (DLP)

	Стахановец	Staffcop
Каналы перехвата	20+	15+
Производительность	✅ Высокая	⚠️ Слабая
ИИ ассистент	✅ Есть	❌ Нет
DLP функционал	✅ Стандартный	✅ Стандартный
Мониторинг сотрудников	✅ Полный	✅ Полный
HR-аналитика	✅ Продвинутая	⚠️ Слабая
Учет времени	✅ Автоматический	✅ Автоматический
Уникальный функционал	ML/AI, анализатор рисков, клавиатурный почерк, голосовое DLP, Антифото	Перехват Windows терминала, командной строки CMD и PowerShell

	Стахановец	Staffcop
Годовая лицензия	От 3699 ₽ От 2590 ₽ (Квант) От 4809 ₽ (Про)	От 5400
Бессрочная лицензия	От 6900 ₽ От 10868 ₽ (ПК) От 14128 ₽ (ПРО)	от 14500

«Стахановец» — единственная российская DLP-система с запатентованными ИИ-технологиями биометрического анализа, превосходящая StaffCop по инновациям при более низкой стоимости

Сравнение с конкурентами

Стахановец

Falcongaze — российская комплексная платформа класса DLP, позиционируется как международный разработчик с фокусом на защиту от внутренних угроз.

	Стахановец	Falcongaze
Производительность	✅ Минимальная нагрузка на ЦП, подходит для слабых компьютеров	⚠️ Требует более мощного оборудования, может замедлять работу системы
ИИ ассистент	✅ Есть	❌ Нет
DLP функционал	✅ Стандартный	⚠️ Создает теневые копии действий, но не всегда блокирует передачу данных
Маркировка скриншотов	✅ Есть	❌ Нет
Геолокация	✅ Даже при включенном VPN	⚠️ Ограниченная функциональность
Голосовое DLP	✅ Есть	❌ Отсутствует или требует внешних сервисов
HR-аналитика	✅ Продвинутая	❌ Нет
Учет времени	✅ Автоматический	✅ Автоматический
Уникальный функционал	ML/AI, анализатор рисков, клавиатурный почерк, Антифото	Темная тема, карта офиса

	Стахановец	Falcongaze
Годовая лицензия	От 3699 ₽ От 2590 ₽ (Квант) От 4809 ₽ (ПРО)	От 8460
Бессрочная лицензия	От 6900 ₽ От 10868 ₽ (ПК) От 14128 ₽ (ПРО)	от 49800

«Стахановец» активно блокирует утечки в реальном времени по всем каналам (включая фото/видео через «Антифото») с помощью ИИ, минимально нагружая инфраструктуру.

Falcongaze SecureTower фокусируется на постфактумном мониторинге действий сотрудников, не обеспечивая проактивной блокировки, особенно от физических способов утечки.

Стахановец

Отстройка от конкурентов

Ключевые особенности

- бесплатная демоверсия Стахановец: ПРО (максимальная редакция) доступна к скачиванию на сайте с автоматической генерацией ключа через Телеграм-бот, доступ на 2 недели
- бесплатный пилот до 30 дней с разверткой на необходимое количество устройств и технической поддержкой для настройки необходимых параметров
- «из коробки» 43 готовых отчета и больше 100 унифицированных настроек, которые можно адаптировать под запрос заказчика
- оперативная реакция технической поддержки на запрос (согласно условиям лицензирования)
- гибкость в вопросах стоимости: широкий набор акционных предложений, несколько редакций под конкретный запрос
- **заказная доработка/разработка под финансово обоснованный запрос**

Стахановец

Отстройка от конкурентов

- **Ключевые особенности**
- Ключевые функции DLP
- Ключевые функции Кадровой аналитики

Ключевые функции DLP

- функция «Антифото»: защита от фотографирования экрана ПК
- функция «Черный ящик»: преобразование скриншотов и записанных звуковых дорожек в видеоролик
- функция «Клавиатурный почерк»: идентификация нетипичного поведения сотрудника по накопленному опыту работы за ПК. **Запатентовано**
- функция «Геолокация»: определение местоположения ноутбуков — внешний IP, страна, город — даже при использовании VPN
- функция «Маркировка»: скрытые цифровые метки на пересылаемые файлы и нанесение watermark на скриншоты
- возможность удаленного выполнения консольной команды на наблюдаемом компьютере незаметно для пользователя
- настраиваемая возможность предотвращения утечки ПДн

Отстройка от конкурентов

- **Ключевые особенности**
- Ключевые функции DLP
- Ключевые функции Кадровой аналитики

Стахановец

Ключевые функции Кадровой аналитики

- **Система кадровой аналитики запатентована**
- автоматизированное профилирование каждого сотрудника по поведению, активности, продуктивности
- сквозная аналитика по всем сотрудникам персонально, по эффективности подразделений
- оценка вовлеченности персонала в работу по заданным метрикам
- дашборды и инфографика с информацией по рабочим и внерабочим активностям в указанное время
- сводный анализ по всем активностям
- интеграция с Outlook и СКУД

Защита сделок

Стахановец

- Необходимо регистрировать сделку при проявлении интереса у заказчика
- Подтверждение или отказ в регистрации придет ответным письмом на почту
- При подтверждении регистрации сделки партнер получает маржу согласно своему партнерскому статусу
- При отсутствии подтверждения регистрации сделка считается не зарегистрированной, соответственно, размер маржи в таком случае составляет 1%, предоставления спец. условий для заказчика отсутствуют

оперативная обработка

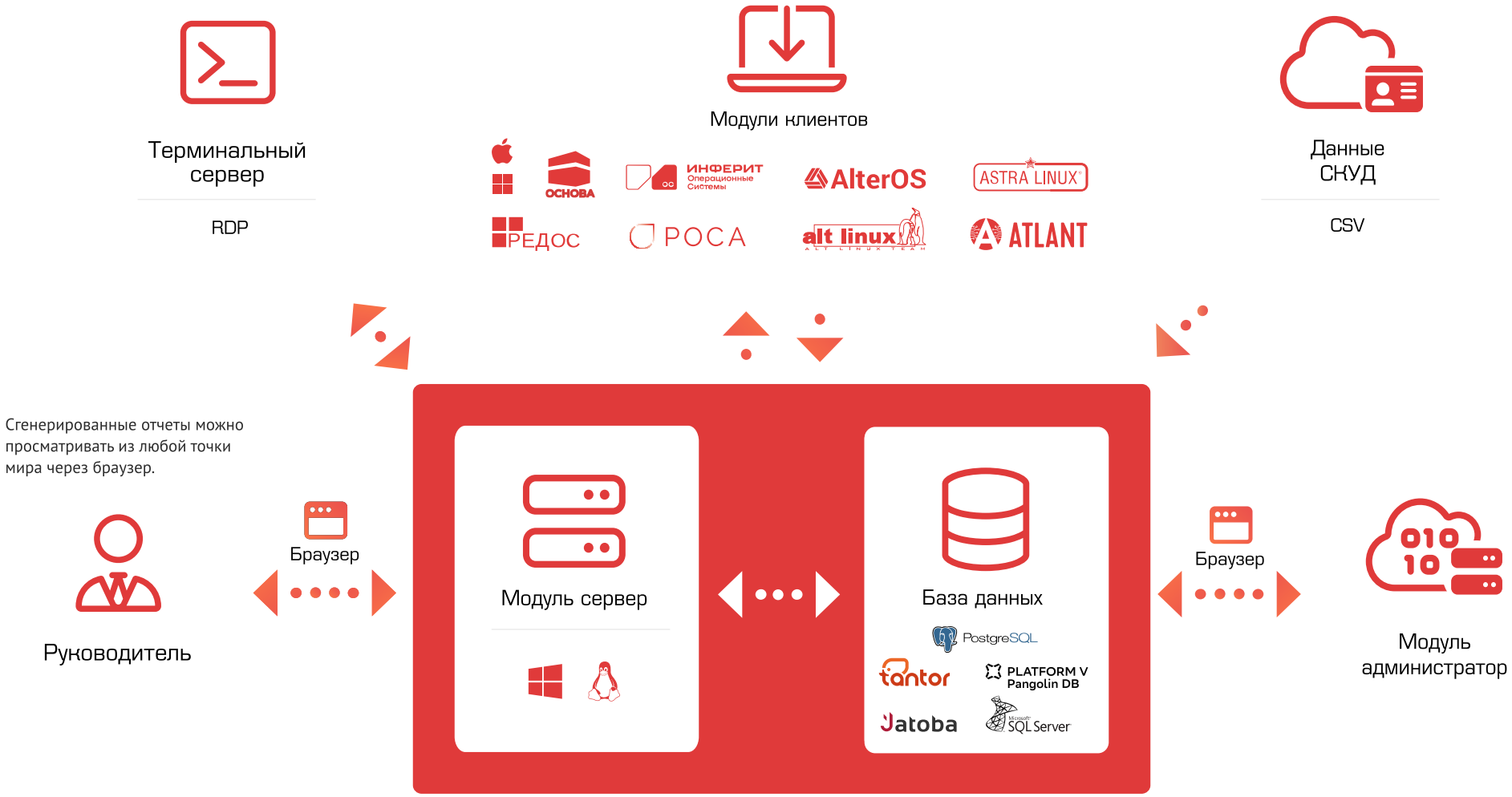
подтверждение менеджером регистрации сделки **гарантирует ее защиту**

зарегистрировать можно **в любой момент**

В случае выполнения условий партнерской программы **возможна доп. мотивация** как для менеджеров, так и для всей компании. Условия обсуждаются индивидуально

Как устроен комплекс: схема работы

Стахановец



Совместимость с отечественным ПО

Стахановец

Сертифицированные ОС:

ИНФЕРИТ Операционные Системы

AlterOS

ASTRA LINUX

РЕДОС

alt linux

ATLANT

ОСНОВА

РОСА

Сертифицированные СУБД:

tantor

Jatoba

Microsoft SQL Server

PostgreSQL

PLATFORM V Pangolin DB

Сертифицированные SEIM:

{KOMRAD} Enterprise SIEM

RUSIEM

Благодаря опции «отправка событий по syslog-протоколу» «Стахановец» может гибко интегрироваться с любыми SIEM-системами, так как предусмотрена возможность передавать во внешнюю систему важные события безопасности

Возможность проведения пилота

Стахановец

ПИЛОТ АБСОЛЮТНО БЕСПЛАТНЫЙ

Мы предоставляем триальные ключи на любое количество лицензий, срок действия лицензий обговаривается.

По завершении пилота просим предоставить отчет о проведения пилота

Демо версия комплекса, которая показывает интерфейс и отчеты комплекса, доступна по ссылке на нашем сайте

Стахановец

Мария Федотова
Ведущий менеджер
по работе с партнерами

stakhanovets.ru

mariya.luts@stakhanovets.ru

+7 (499) 110-64-10

визитная карточка

123112, Москва, деловой центр «Москва-Сити», Пресненская наб., 12, Башня Федерация Восток, 49 этаж, офис 17
ООО «Стахановец», ИНН: 7725836290; ОГРН: 1147746831220