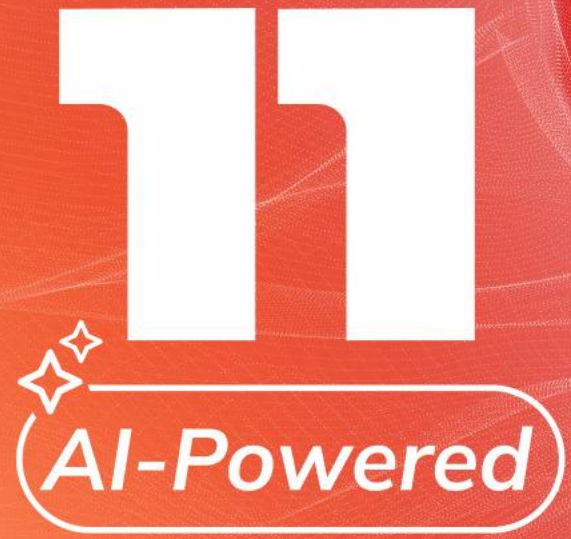
Стахановец

От угроз к возможностям: Использование DLP для стратегического управления рисками



Программный комплекс Стахановец

stakhanovets.ru

Стахановец

Стахановец

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

16 лет
на ИТ-рынке России

21 000
внедрений в РФ и других странах

11 версия
программного продукта

Российский продукт

Внесен в Единый реестр российского ПО МинЦифры

Патенты РФ

Разработки «Стахановец» запатентованы

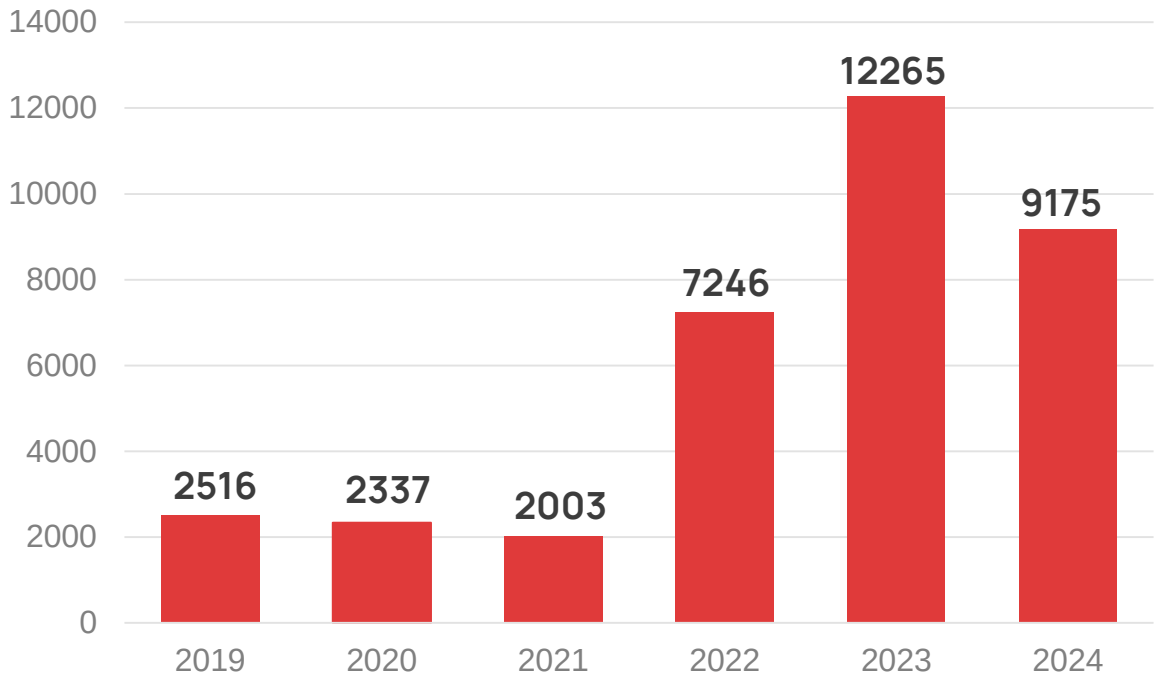
Лицензия ФСТЭК

На деятельность по разработке и производству СЗИ

Динамика зарегистрированных утечек информации в мире

Стахановец

Мир



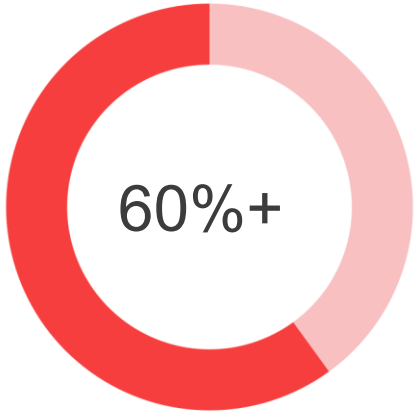
В 2024 году среди утечек внутреннего характера на случайные нарушения пришлось 52,8%, на умышленные 47,2%.

* По данным отчета InfoWatch «Утечки информации в мире 2023-2024 годы»

Масштаб внутренней угрозы

Стахановец

Инциденты, инициированные изнутри компании, обходятся бизнесу значительно дороже внешних атак — и наносят ущерб не только финансовый, но и репутационный.

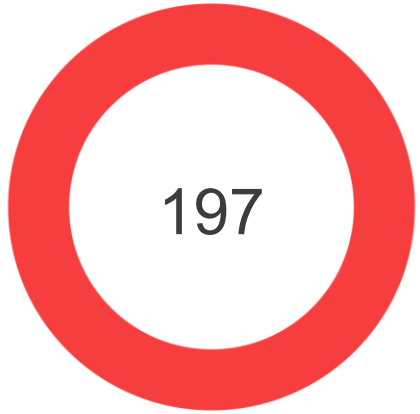


Утечек изнутри

В 2025 году более 60% утечек данных в мире инициированы действиями сотрудников — умышленно или по халатности

Средний ущерб

Средняя стоимость инцидента с участием инсайдера превышает ущерб от типичной внешней кибератаки



Дней до обнаружения

Среднее время выявления внутренней утечки — почти полгода незамеченного ущерба

*Согласно аналитическому отчету IBM & Ponemon Institute "Cost of a Data Breach" и прогнозам Gartner, 2025

Проблемы и риски бизнеса

Стахановец

- Рост числа внутренних нарушителей в организациях
- Рост числа атак на ИТ-инфраструктуру на фоне геополитики и новых законов
- Серьезные финансовые риски для компаний
- Доступность киберуслуг на черном рынке
- Текучесть персонала и дефицит кадров на рынке труда
- «Хактивизм» как спонтанное движение для выражения своей позиции

Внутренний нарушитель как причина утечек информации

Стахановец

ИНСАЙДЕР — это лицо, которому доверен и предоставлен доступ к конфиденциальной информации

Два типа внутренних нарушителей:

- Неумышленный нарушитель
- Умышленный нарушитель

За последние 3 года наблюдается рост обеих категорий внутренних нарушителей, но в большей степени — **рост целенаправленных утечек**

Кейс 1: Охота за головами

Стахановец

Михаил Петров, 43 года
Ведущий авиадиспетчер

Промышленный шпионаж
Переманивание персонала конкурентами

15 млн ₽
предотвращено

14 дней
на выявление

94 %
риск ИИ

Индикаторы угрозы

- Поиск работы в рабочее время
- Копирование 2,3 ГБ данных партнёров
- Аномальная активность в мессенджерах
- Запросы к внутренним регламентам

Кейс 1: Как помогла DLP-система

Стахановец

Проактивное выявление риска утечки

Мониторинг действий

- Посещение HH.ru и карьерных сайтов
- Скачивание и копирование конфиденциальных данных
- Анализ активности в мессенджерах (Telegram)

Результат:

- Сотрудник сохранён благодаря своевременному диалогу
- Утечка коммерческой тайны предотвращена
- Выявлена схема переманивания

Кейс 2: Ночной торговец данными

Стахановец

Елена Васильева, 32 года
Инспектор службы безопасности

Продажа персональных данных пассажиров

75 млн ₽
потенциальный штраф

8 месяцев
длительность схемы

87 %
риск ИИ

Индикаторы угрозы

- Ночной доступ к данным пассажиров через VPN
- Массовое создание скриншотов
- Подозрительная переписка в WhatsApp
- Несоответствие доходов и трат

Кейс 2: Как помогла DLP-система

Стахановец

Выявление внутреннего нарушителя

Мониторинг действий

- Контроль доступа к ПДн в нерабочее время
- Лингвистический анализ переписки
- Сопоставление с финансовыми операциями

Результат:

- Задержание с поличным в ходе операции «Skyfall»
- Предотвращена утечка данных 50 000 пассажиров
- Пресечена деятельность преступной группы

Сколько стоит работа с сотрудниками?

Стахановец

25% Текучесть кадров в России в 2025 году

68% ресурсов HR тратится на найм, только 17% на удержание

30%

крупных компаний столкнулись с критическим уровнем текучки

77%

компаний фиксируют негативное влияние выгорания

57%

сотрудников работают на пределе возможностей

Кейс №1 — FlightRisk

Стахановец

Предотвратили увольнение ключевого разработчика

Ситуация: ИИ выявил риск ухода 0,78 (высокий!) в течение 30-45 дней

Драйверы риска:

- Стагнация роста
- Дисбаланс вклада и признания
- Перегрузка задачами

План действий ИИ:

- 72 часа: Stay-интервью, публичное признание (+10% за менторство)
- 30 дней: KPI за ревью, карьерная дорожная карта на 6 месяцев
- 2 месяца: Компенсация +8-12%, регулярные 1:1

Результат:

Сотрудник остался, мотивация выросла

Кейс №2 — Цифровой надзор: эволюция контроля в финансах

Стахановец

О заказчике:

Компания: Крупный федеральный финансовый холдинг

Масштаб: Разветвлённая сеть по всей России, тысячи сотрудников (офис + удалёнка)

Среда: Высокая конкуренция и жёсткое госрегулирование

Цели и задачи:

Традиционные KPI давали лишь итоговую картину, но не отвечали на ключевые вопросы руководства:

Анализ операционной эффективности: как выявить и устранить скрытые потери рабочего времени и ресурсов, которые приводят к росту себестоимости и срывам сроков при формальном выполнении плановых показателей?

Управление кадровым потенциалом, затратами и лояльностью: как снизить операционные расходы на персонал (переработки) и уменьшить текучесть кадров, если формальные показатели выполнения планов не выявляют проблем?

Оптимизация рабочей модели: на каких принципах (офис/удаленка/гибрид) должна строиться работа каждого подразделения, чтобы максимизировать продуктивность при минимальных затратах?

Проактивное управление, риски, связанные с персоналом: как создать систему раннего обнаружения выгорания, демотивации и нелояльности предотвращения финансовых потерь и инцидентов информационной безопасности?

Кейс №2 — Решение

Стахановец

Финансовой организации требовался не просто инструмент контроля, а **система управленческой аналитики**, которая превратила бы цифровые следы сотрудников в понятные бизнес-инсайты для принятия решений.

Решение:

Финансовая организация, уже использующая DLP-систему «Стахановец» для базовой защиты, обратилась к экспертам с запросом на расширение ее функционала.

Цель — настроить DLP «Стахановец» для глубокого анализа продуктивности и выявления закономерностей.

Вместе со специалистами партнера была разработана и внедрена программа аналитики на базе DLP «Стахановец», в рамках которой была протестирована серия гипотез о связи поведения сотрудников с бизнес-результатами.

Система была настроена на сбор обезличенных данных активности персонала, использованию приложений, режиму работы с привязкой к структурным единицам (трайбам, дирекциям).

Кейс №2 — Результаты

Стахановец

Внедрение аналитического подхода на базе DLP «Стахановец» привело к **конкретным бизнес-результатам:**

Для руководства компании:

Обоснование модели работы: Появились фактические данные для принятия решений о том, как организовать работу каждого подразделения в офисе, удаленно или в смешанном формате, для повышения общей эффективности.

Контроль над процессами: Исчез «слепой» участок между задачей и итогом. Руководство видит реальную загрузку, распределение времени и вовлеченность сотрудников, что позволяет управлять ресурсами обоснованно.

Снижение бизнес-рисков: Система позволяет заранее выявлять зоны низкой эффективности, потенциального срыва сроков и сотрудников с признаками выгорания, помогая предотвращать убытки.

Для HR-департамента:

Превентивная работа с выгоранием: Снижение необоснованных переработок и точечная работа с сотрудниками в зоне риска.

Снижение текучести: Раннее выявление снижения вовлеченности позволило сохранить ценные кадры.

Объективная оценка нагрузки: Данные для корректного планирования штата и распределения задач..

Для Службы ИБ:

Контекст для расследований: аналитика продуктивности добавила контекст к событиям безопасности, помогая отличить злонамеренные действия от ошибок, вызванных перегрузкой или неэффективными процессами.

Кейс №2 — Отзыв клиента

Стахановец

Этот кейс демонстрирует, что современная DLP-система — это платформа для решений на основе данных, способная отвечать не только на вопрос «что случилось?», но и на более важный — «почему это произошло и как это предотвратить?», принося прямую бизнес-ценность.

«

Раньше мы видели лишь вершину айсберга — итоговые цифры по KPI и отчеты руководителей. Всё, что происходило в процессе работы, оставалось за кадром: реальная загрузка команд, разница между офисом и удалённой работой, истинные причины переработок и выгорания.

Развернув аналитические возможности «Стахановца» вместе с партнерами мы, наконец, увидели полную картину. Система предоставила нам не просто данные об активности, а настоящие бизнес-инсайты.

Например, мы доказали, что эффективная удалённая работа возможна, но требует особого управления задачами. Мы научились вычислять сотрудников на грани выгорания за месяцы до увольнения и точечно работать с ними. Мы получили объективный инструмент для оценки влияния организационной культуры разных трайбов на результаты.

Теперь наша HR-политика и решения по оптимизации процессов основаны не на интуиции, а на данных. DLP «Стахановец» для нас перестала быть просто элементом ИБ-ландшафта. Это стратегическая платформа для управления эффективностью и человеческими ресурсами, которая уже показывает измеримую ценность.

»

— Руководитель направления по аналитике данных и продуктивности, крупная финансовая организация.

Кейс №2 — Почему это решение подойдет Вам?

Стахановец

Собственники и топ-менеджмент:

Получите полную прозрачность бизнес-процессов и фактические данные для оценки реальной эффективности инвестиций в персонал и цифровые ресурсы.

Руководители департаментов и ключевых направлений:

Перейдите от управления на основе отчётов к управлению на основе данных. Выявляйте точки роста, находите внутренние резервы и объективно оценивайте результативность подразделений.

Директор по персоналу:

Создайте систему превентивного управления кадрами. Предотвращайте профессиональное выгорание, снижайте текучесть и формируйте культуру высокой продуктивности, основанную на объективных метриках.

Директор по информационной безопасности:

Дополните мониторинг ИБ-инцидентов аналитикой человеческого фактора. Управляйте не только угрозами информационной безопасности, но и поведенческими рисками, связанными с действиями сотрудников.

Сделайте аналитику поведения сотрудников ключевым инструментом для повышения эффективности и прибыльности бизнеса

Кейс №2 — Используемые инструменты

Стахановец

Аналитический модуль DLP «Стахановец» позволил перейти от наблюдения к пониманию:

1. **Сравнение форматов работы:** Система наглядно показала, что удаленные сотрудники при четких KPI демонстрируют более высокую активность и гибкость графика, в то время как офисный формат обеспечивает стабильность.
2. **Диагностика переработок и выгорания:** была выявлена прямая корреляция - систематические переработки ведут к снижению эффективности и повышению риска невыполнения планов. Это позволило HR вмешиваться точечно.
3. **Раннее предупреждение увольнений:** анализ подтвердил, что уволившиеся сотрудники за месяцы до ухода резко снижали активность. DLP «Стахановец» стала системой раннего оповещения для службы по работе с персоналом.
4. **Оценка влияния руководителей:** данные показали, что в эффективных дирекциях с сильным лидерством общая активность и дисциплина команды значительно выше. Это дало инструмент для оценки работы менеджмента.
5. **Контроль дисциплины и инструментов:** выявлено, что прогулы и постоянное переключение между десятками приложений серьезно снижают общую продуктивность отдела.

Сочетание простоты
и широких возможностей

Стахановец

- минимальные требования к оборудованию
- простое внедрение и обслуживание
- совместимость с антивирусным ПО
- масштабируемость на 35 000+ АРМ
- оперативная техподдержка

Стахановец

stakhanovets.ru

+7 (499) 110-64-10

info@stakhanovets.ru

@STAKHANOVETS_RU

Наш Телеграм-канал с новостями
из мира информационной безопасности и
Employee Monitoring

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

2025.10