

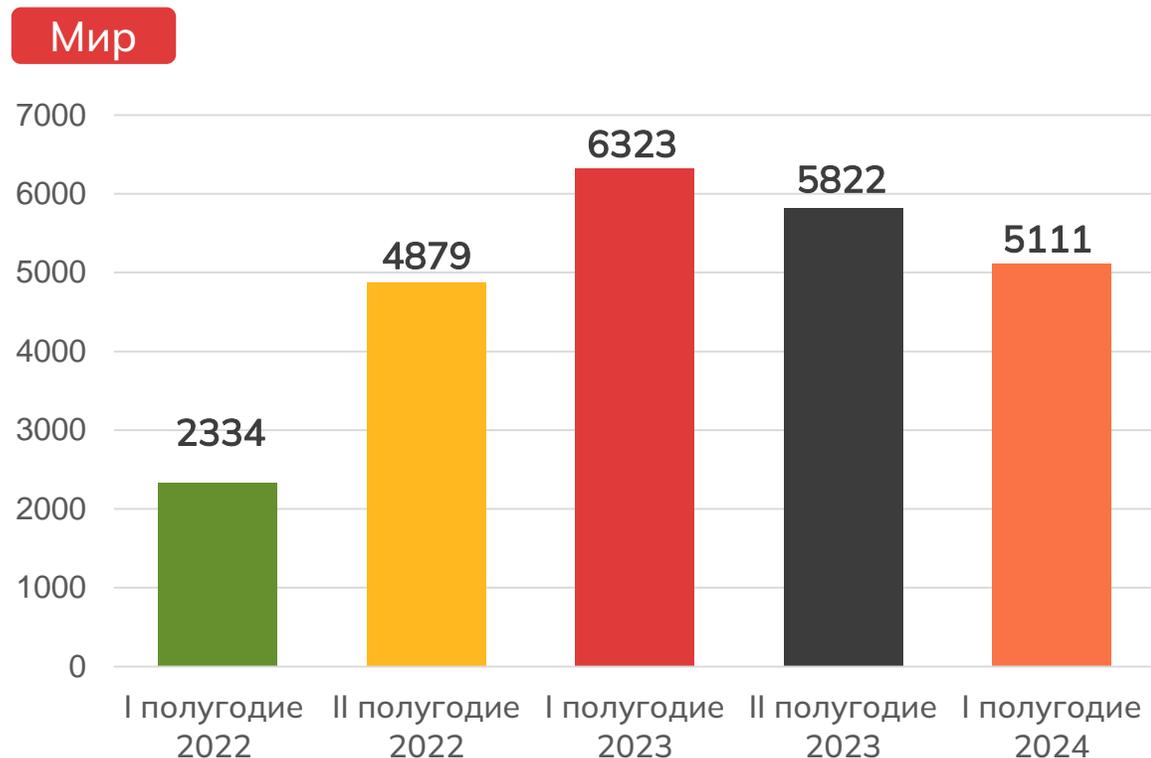


УПРАВЛЕНИЕ ВНУТРЕННИМИ РИСКАМИ, РЕАЛИИ СОВРЕМЕННОГО МИРА

stakhanovets.ru



Динамика зарегистрированных утечек информации в мире, 1Н-2024



Согласно аналитическому отчету компании Infowatch (2024), среди утечек внутреннего характера к умышленным инцидентам относится **более 89%**

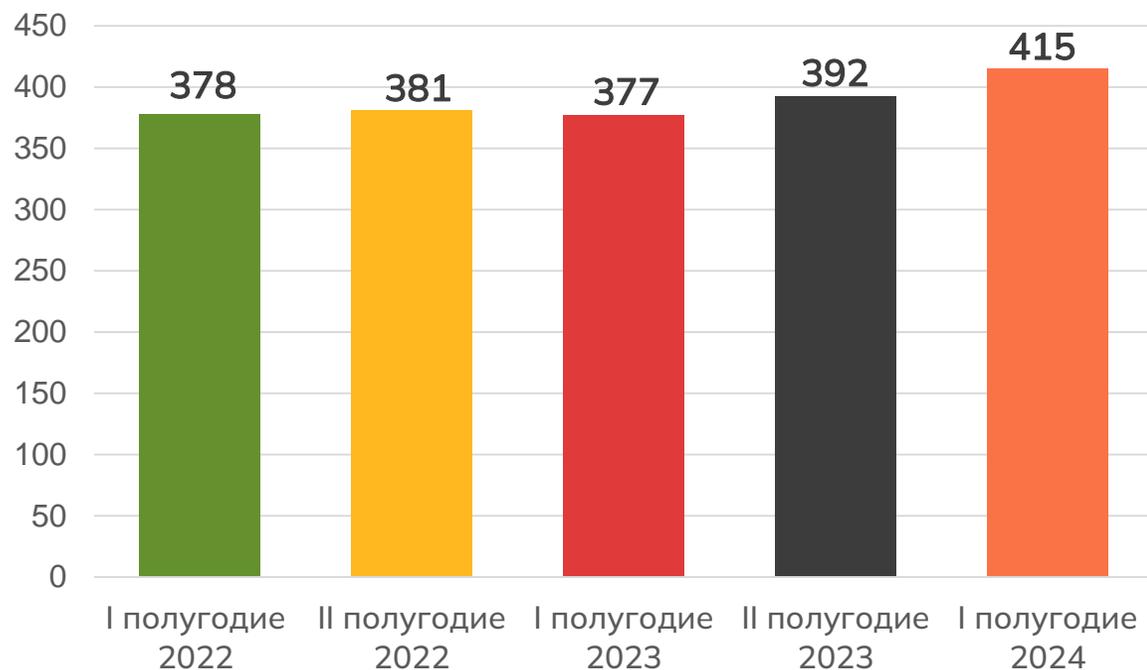
* Согласно аналитическому отчету infowatch, 2024

Проблемы и риски бизнеса в России

- Рост числа инсайдеров в организациях
- Рост числа атак на ИТ-инфраструктуру на фоне геополитики и новых законов
- Ужесточение наказаний за утечки персональных данных и серьезные финансовые риски для компаний
- Доступность киберуслуг на черном рынке
- Текучесть персонала и дефицит кадров на рынке труда
- Хакер-«активизм» как спонтанное движение для выражения своей позиции

Динамика зарегистрированных утечек информации в РФ, 2022-2024

Россия



Количество утечек в мире в 1ПГ-2024 **сократилось на 19%**, а в России — **выросло на 10%**

Всего за 1ПГ-2024 в РФ утек антирекордный **1 МЛРД. ЗАПИСЕЙ ПДН.**

* Согласно аналитическому отчету infowatch, 2024

>66%

Утечек совершается по вине
сотрудников компании

Кейс: «Мегаляп» МЕТА *

Год: 2024

\$34,146 В

выручка в Q3 2023

\$1,22 Т

рыночная стоимость в 2023

*ПРИЗНАНА ЭКСТРЕМИСТСКОЙ И ЗАПРЕЩЕНА В РФ

stakhanovets.ru

Customer Experience:

- бывший вице-президент Meta* при увольнении выкрал конфиденциальные документы компании
- в иске говорится, что бывший вице-президент по инфраструктуре Дипиндер Сингх Хурана, подав заявление об уходе, похитил файлы с внутренней информацией о дата-центрах, поставщиках и проектах, связанных с технологиями ИИ. Также в документах были данные о бизнес-операциях и расходах, связанных с закупками
- внутренние файлы бывший топ-менеджер загрузил на личный Google Drive и Dropbox, после чего многие документы были скопированы в папки с именем нового работодателя

ССЫЛКА НА МАТЕРИАЛЫ: [BLOOMBERG.COM](https://www.bloomberg.com)

Инсайдер как причина утечек информации



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

Два типа инсайдеров-нарушителей:

- Неумышленный нарушитель
- Умышленный нарушитель



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



Insider Risk Management (IRM) — это метод управления рисками, связанными с внутренними угрозами в организации

IRM — это процесс выявления, оценки и смягчения рисков, связанных с действиями сотрудников, подрядчиков или других внутренних участников организации, которые могут намеренно или случайно причинить вред компании. Эти риски могут включать утечку конфиденциальной информации, кражу интеллектуальной собственности, саботаж, мошенничество и другие виды угроз.

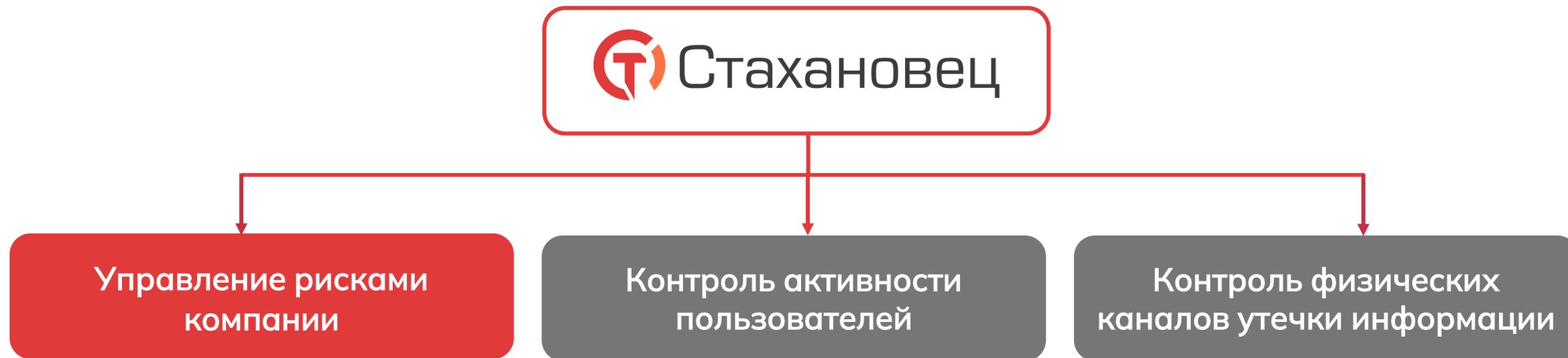


Функции:

- анализ поведения
- выявление рисков
- фиксация действий
- защита данных
- реагирование на инциденты

Цель IRM — обеспечить безопасность компании и её активов от внутренних угроз и минимизировать риски, связанные с деятельностью сотрудников внутри организации

Как усилить безопасность в компании?



**МНОГОФУНКЦИОНАЛЬНОЕ РЕШЕНИЕ,
ОСНОВАННОЕ НА ДАННЫХ О ПОВЕДЕНИИ СОТРУДНИКОВ ЗА РАБОЧИМ МЕСТОМ**

Предотвращение сговора и коррупционных схем



Основные риски для бизнеса:

- Экономические преступления на коммерческих позициях
- Прекращение деятельности бизнеса
- Отсутствие доказательной базы для отстаивания прав



Основные заинтересованные сотрудники:

- Руководители всех уровней
- Отдел по борьбе с экономическими преступлениями (ОБЭП)
- Отдел комплаенса и юридическая служба

Как комплекс предотвращает риски?



Анализатор рисков
и рейтинг рисков



Выявление
отклонений
от нормы



Регулярные
Отчеты
на почту



Анализ
взаимодействий

Кейс: Сговор и «слив» баз

Год: 2019

Судебный прецедент

Результат: выигрыш
по делу работодателем

Данные о судебном иске:

Бажин М.С. против транспортно-экспедиционной
компании «Моно Транс-Строй»

Увольнение по ТК РФ ст.81 за разглашение охраняемой
законом тайны (коммерческой)

Программа Стахановец выявила:

- 6 000 файлов было скопировано на USB-флеш-носитель
- через Viber передавались коммерческие данные
о клиентах и заказах
- удален файл базы данных MySQL с информацией
за 5 лет 2014-2019 гг.

Контроль репутационных рисков



Основные риски для бизнеса:

- Репутационные риски и последующие финансовые издержки
- Незаконные действия сотрудников
- Отсутствие доказательной базы для отстаивания прав



Основные заинтересованные сотрудники:

- Руководители всех уровней
- Отдел комплаенса и юридическая служба
- Отдел маркетинга и PR

Как комплекс предотвращает риски?



Фиксация действий сотрудников в виде готовых отчетов



Развитая система хранения данных, поиска и отчетов



Логирование экрана и оптимизация скриншотов

Кейс: Кража гостайны

Год: 2018

Судебный прецедент РФ

Результат: уголовное наказание
в виде штрафа, подписка о невыезде

Данные о судебном иске:

Уголовное дело в отношении Коробейникова А.И.
по причине несанкционированного доступа
и кражи данных у ФГУП «ГЦСС» - Спецвязь

УК РФ ч.1 ст.183, УК РФ ч.1 ст. 272

Программа Стахановец позволила:

- выявить несанкционированное логирование в электронную почту госпредприятия с нового рабочего места (зафиксировано скриншотами)
- оперативно обнаружить нарушение закона и выявить виновного
- передать данные Федеральной Службе Безопасности

Проактивная защита от утечек



Основные риски для бизнеса:

- Утечка критических данных
- Промышленный шпионаж
- Разглашение конфиденциальной информации



Основные заинтересованные сотрудники:

- Руководители всех уровней
- Служба безопасности (СБ)
- Служба информационной безопасности (ИБ)

Как комплекс предотвращает риски?



Запрет отправки важных документов



«Водяные знаки» (watermarks) на изображениях



Маркировка документов и цифровые отпечатки



Поиск по файлам на клиентской машине (Краулер)



Контроль печати



Распознавание текста на скриншотах (OCR)

Кейс: Конкурентный переход

Год: 2021

Судебный прецедент

Результат: выигрыш
по делу работодателем

stakhanovets.ru

Данные о судебном иске:

Ларина Н.А. против ОАО «Научно-исследовательский и проектный институт карбамида» (ОАО «НИИК»)

Увольнение по ТК РФ ст.81 за разглашение охраняемой законом тайны (коммерческой)

Программа Стахановец позволила:

- копирование данных коммерческой тайны и технологической информации под NDA на USB-флеш-носитель
- отправку резюме в конкурирующую структуру
- последующее за этим разглашение данных ОАО «НИИК»

Контроль криптоактивов



Основные риски для бизнеса:

- Несанкционированные криптопереводы в контуре компании
- Репутационные риски и последующие финансовые издержки
- Мошеннические действия



Основные заинтересованные сотрудники:

- Отдел по борьбе с экономическими преступлениями (ОБЭП)
- Служба безопасности (СБ)
- Руководители всех уровней
- Отдел маркетинга и PR

Как комплекс предотвращает риски?



Перехват адреса
криптокошелька
в буфере обмена

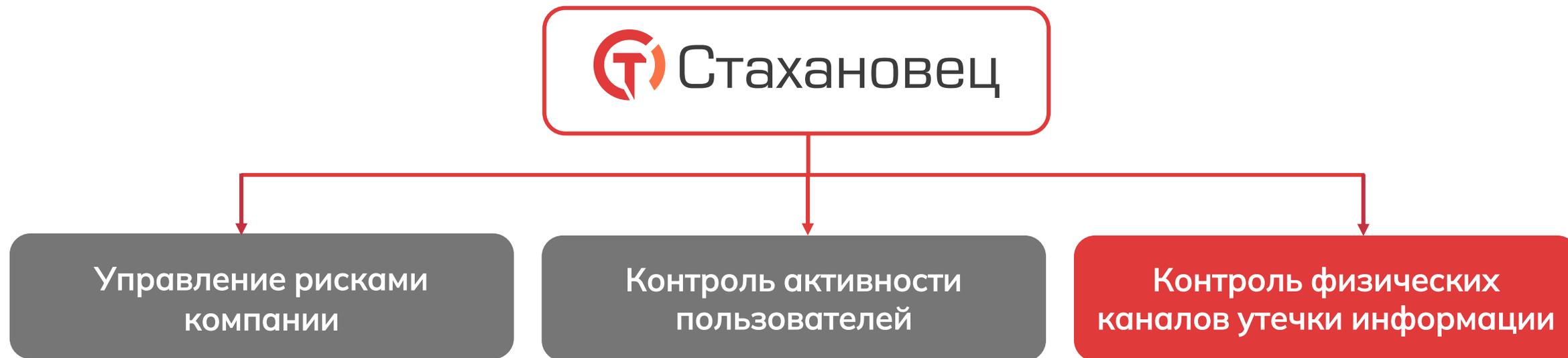


Автоматическая
проверка на
благонадежность



Интеграция
с платформой
ШАРД

Как усилить безопасность в компании?



**МНОГОФУНКЦИОНАЛЬНОЕ РЕШЕНИЕ,
ОСНОВАННОЕ НА ДАННЫХ О ПОВЕДЕНИИ СОТРУДНИКОВ ЗА РАБОЧИМ МЕСТОМ**

Кейс: Депремирование за порнофилию

Год: 2019

Судебный прецедент

Результат: выигрыш
по делу работодателем

Данные о судебном иске:

Хайбуллина Р.Р. против ПАО «Башинформсвязь»

Гражданское дело: оспаривание годового депремирования
и наложения дисциплинарного взыскания

Программа Стахановец позволила:

- восстановить веб-историю посещений сотрудника в сети Интернет с корпоративного ПК
- выявить посещение 39 сайтов не по рабочей теме, включая онлайн-порно-хостинг
- выиграть иск

Каналы утечки информации



Средства
коммуникации



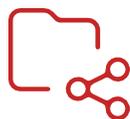
Флешки и другие
съемные носители



Скриншоты и фото
ценных документов



Средства печати
документов



Общие
файловые ресурсы

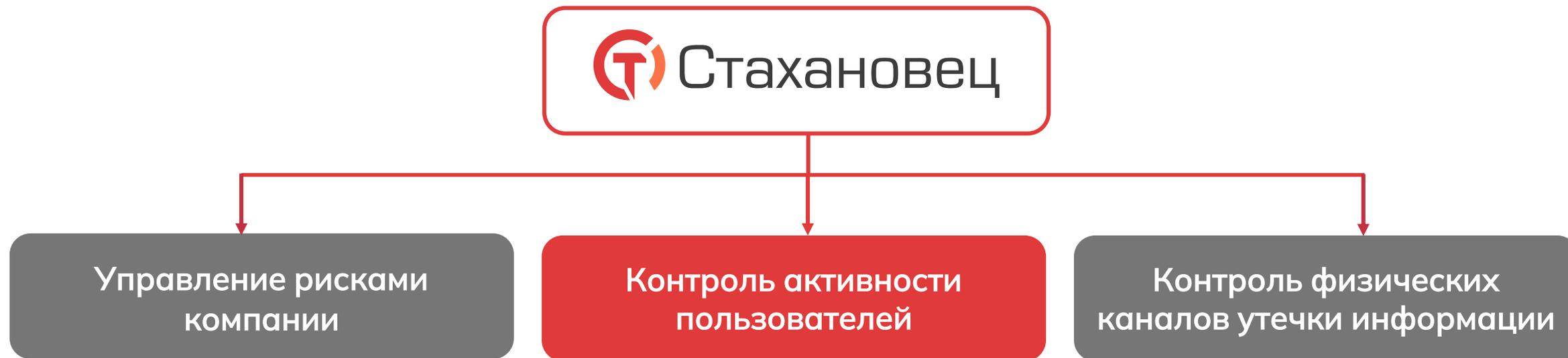


Сервисы публикации
(веб-ресурсы)



Доп. риски: удаленный доступ
и конфликт внутренних политик

Как усилить безопасность в компании?



**МНОГОФУНКЦИОНАЛЬНОЕ РЕШЕНИЕ,
ОСНОВАННОЕ НА ДАННЫХ О ПОВЕДЕНИИ СОТРУДНИКОВ ЗА РАБОЧИМ МЕСТОМ**

Расширение инструментов для обеспечения безопасности

Стахановец можно использовать не только как самостоятельный инструмент, но в дополнение к другим DLP-решения



Контроль физических каналов утечки информации

- Система Антифото — контроль и предупреждение попыток сфотографировать экран компьютера на камеру смартфона
- Распознавания лиц с веб-камеры — возможность автоматической идентификации сотрудников: запись снимков с веб-камер машин сотрудников и сохранение на сервере для дальнейшего детального анализа в случае расследования инцидентов



Контроль активности пользователей

- Контроль инсайдеров
- Мониторинг поведения сотрудников за рабочим местом (онлайн и оффлайн наблюдение)
- Выявление нелояльных сотрудников (анализатор рисков, кадровая аналитика)
- Системный анализ поведения пользователей (сводный отчет, аналитика, лента активности)

Как устроен комплекс: схема работы



Наши основные преимущества для вашего предприятия



низкие системные требования
к серверной части и АРМ



простое внедрение
и обслуживание



совместимость
с антивирусным ПО



масштабируемость
на 35 000+ АРМ



оперативная
техподдержка

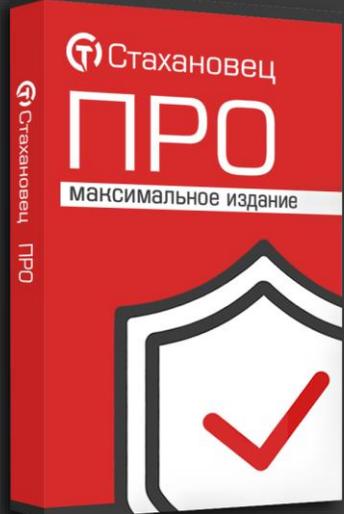
Программные инструменты

₽ ₽



Полный контроль — DLP-комплекс для предотвращения утечек данных. Возможности системы позволяют находить инсайдеров, а в случае утечки — проводить расследования

₽ ₽ ₽



ПРО — максимальное издание программного комплекса, включающее в себя все функции Кванта, Полного Контроля и уникальные опции анализа и DLP

₽



Квант — инструмент поведенческого и сравнительного анализа подразделений, с возможностью генерации резюме по каждому сотруднику

Стахановец

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



Официальный
резидент
Сколково

↗ 15 лет

на ИТ-рынке России с 2009 года

↗ 19 000

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



Сертификат ФСТЭК

4-й уровень доверия

Нас выбирают



↗ 2 МЛН

АРМ под наблюдением
ПО Стахановец



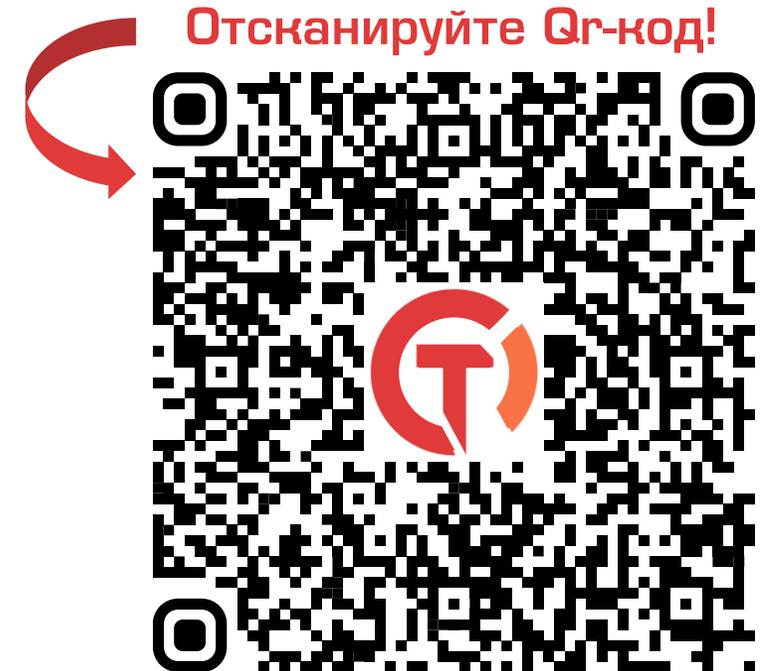
Акция 

Для участников мероприятия

 Стахановец

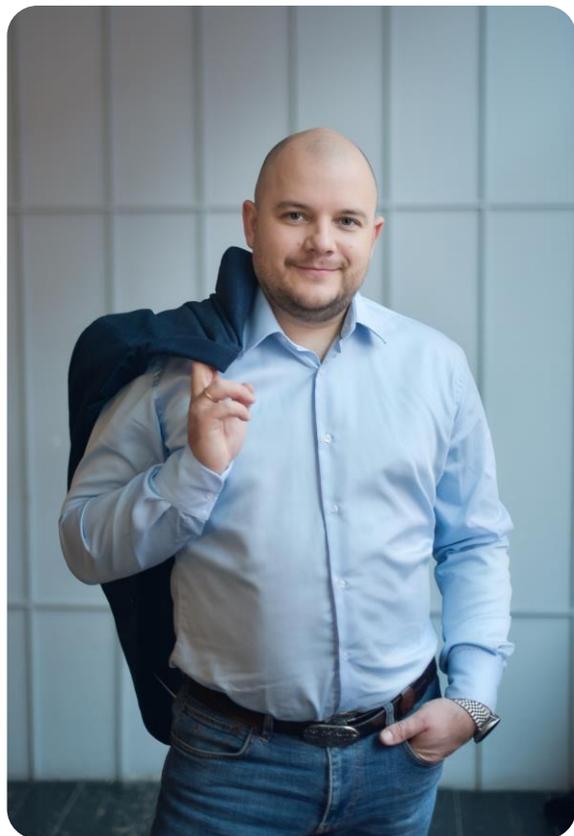
Скидка 20%

**на покупку
«Стахановец» ПРО**



СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?



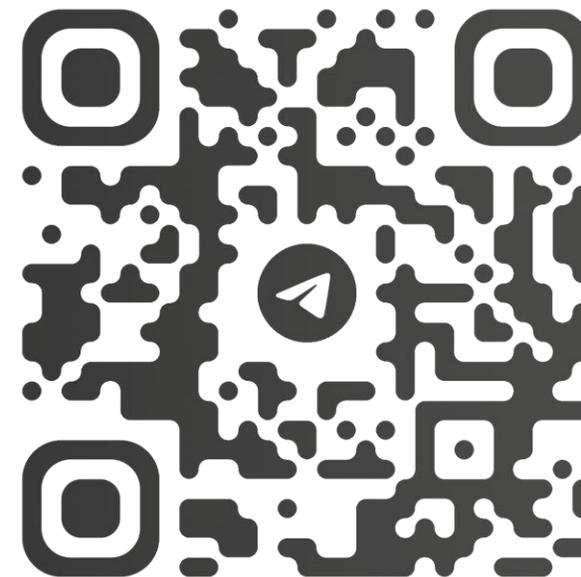
Артём Жадеев
Директор по продажам

 stakhanovets.ru

 info@stakhanovets.ru

 +7 (499) 110-64-10

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



@STAKHANOVETS_RU