staffcop®

Расследование инцидентов
внутренней безопасности

Хорошо информированные и безопасные: кейсы расследования ИБ в цифровой эпохе

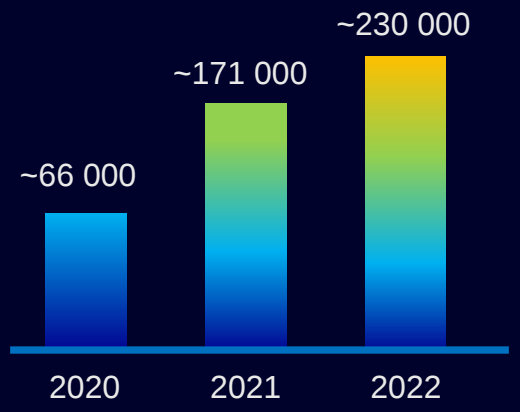
Станислав Юдинских

Менеджер проектного офиса
ООО Атом Безопасность
s.yudinskikh@staffcop.ru

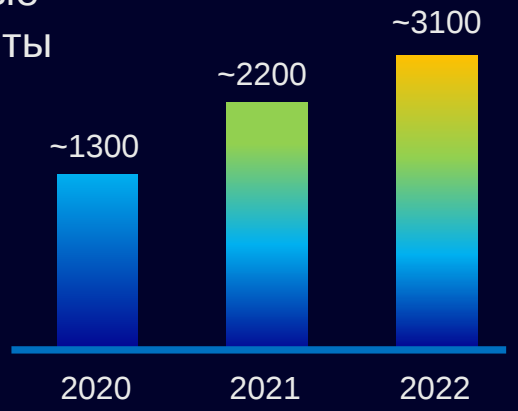
О компании

staffcop

ARM
+35%



Серверные компоненты
+40%



20+

Клиентов из списка Топ-100 Forbes

90+

Сотрудников

200

Конференций, в которых мы приняли участие за 3 года

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

4-й уровень доверия

Импортонезависимый продукт
Российский разработчик

СКБ Контур

АРПП
Отечественный софт

Минцифры России

Участник

академпарк

Решаемые задачи

staffcop

Информационная безопасность

- Раннее обнаружение угроз ИБ
- Расследование инцидентов
- Анализ поведения пользователей

Эффективность работы персонала

- Оценка продуктивности сотрудников
- Мониторинг бизнес – процессов
- Учет рабочего времени

Администрирование рабочих мест

- Удаленное администрирование
- Инвентаризация компьютеров
- Индексирование файлов на ПК

Для кого?

Собственников бизнеса

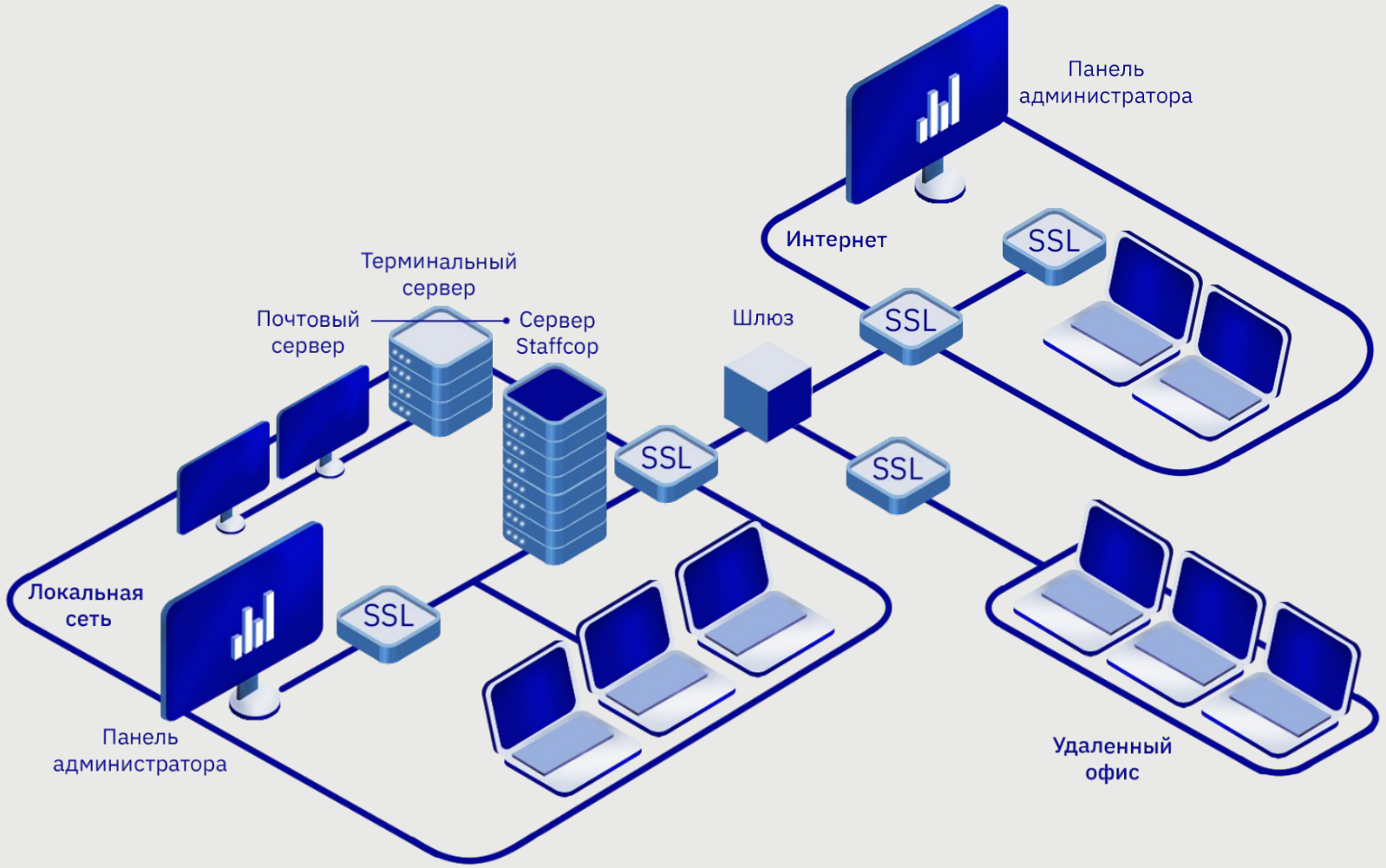
IT специалистов

ИБ специалистов

Сотрудников HR

Современные архитектурные решения

- Единая веб-консоль
- 100 ПК <=> 6 CPU, 32 RAM
  1000 ПК <=> 12 CPU, 96 RAM
- Для работы достаточно одного виртуального сервера
- Агент для Windows, Linux, macOS
- Минимальные требования к железу
- Импортнезависимое ПО
- Масштабируемая архитектура
- OLAP технология хранения данных



staffcop

staffcop®

Кейсы
Восемь случаев на мониторе: уроки из мира кибербезопасности

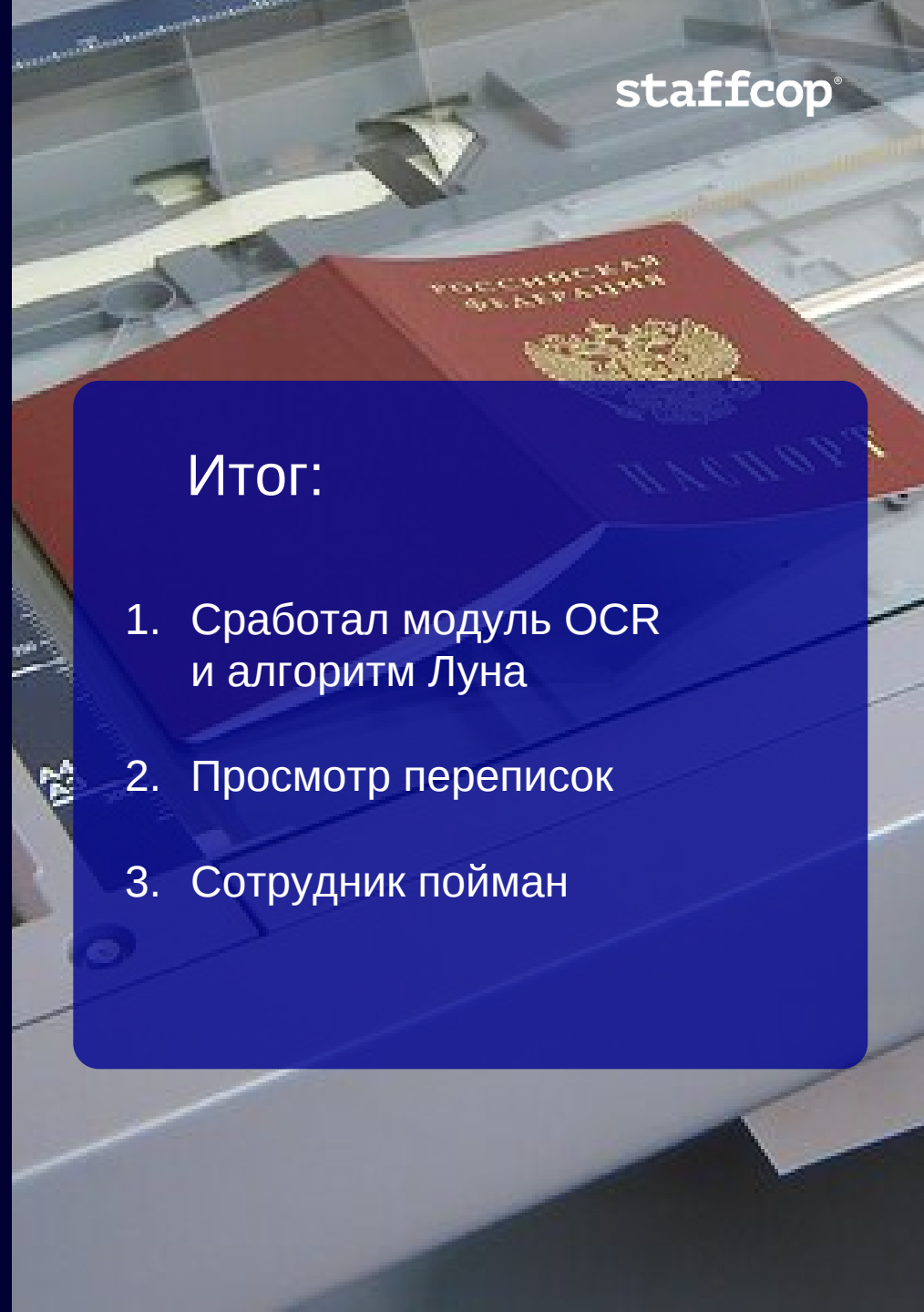
Утечка скана паспорта и номера карты (Банк, 500 ПК)

1. Кто: Сотрудница банка

1. Отправила с личной почты и через мессенджеры сканы паспорта и номер карты клиента

1. Пыталась передать третьему лицу для мошеннических действий

1. Что грозило компании: репутационные риски и нарушение предписаний регуляторов, штрафы

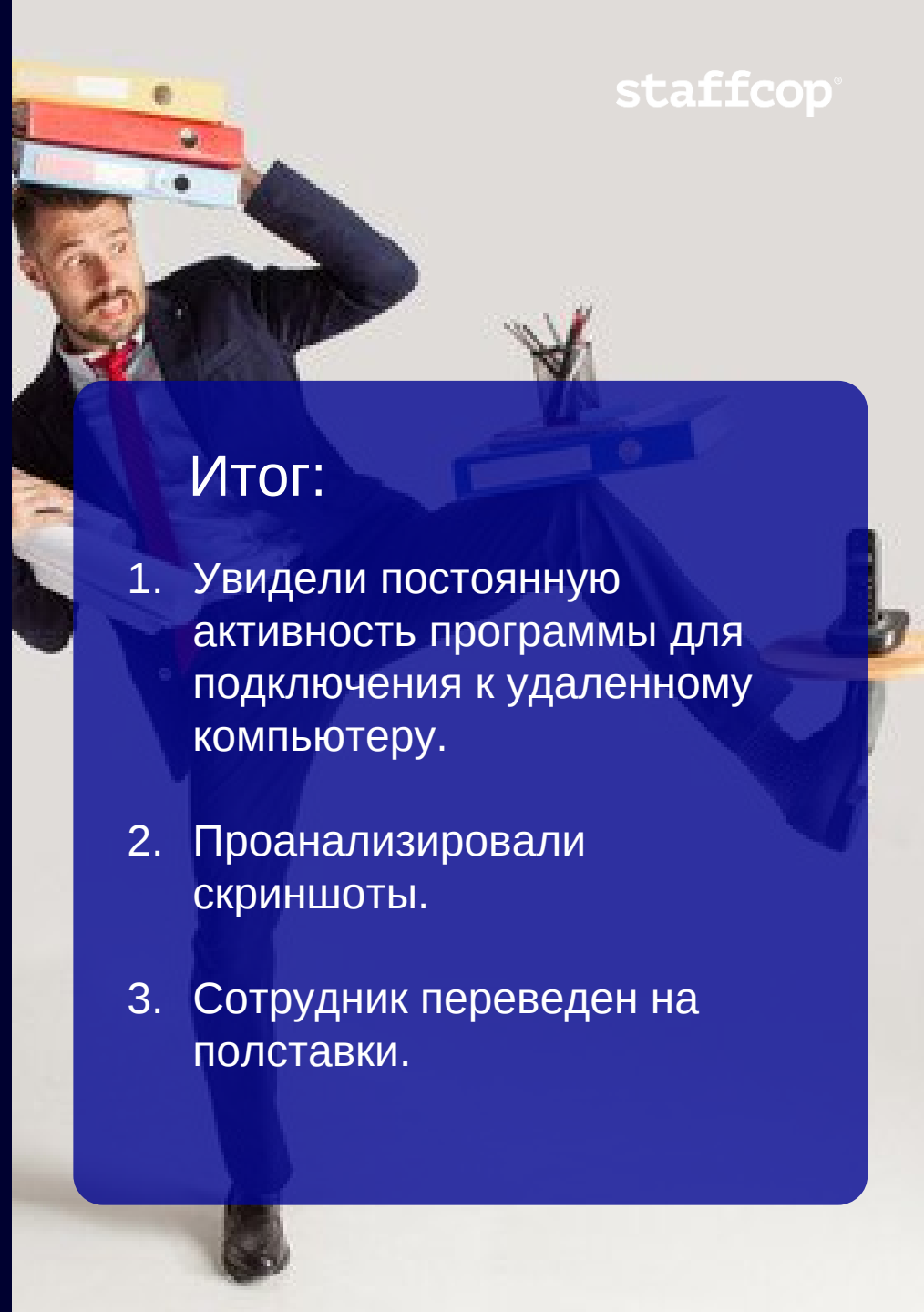


Итог:

1. Сработал модуль OCR и алгоритм Луна
2. Просмотр переписок
3. Сотрудник пойман

Параллельный бизнес

1. Кто: опытный бухгалтер
1. Резко понизилась продуктивность опытного сотрудника
1. Подключалась к удаленному компьютеру у себя дома.
1. Параллельно занималась делами своего ЮЛ.



Итог:

1. Увидели постоянную активность программы для подключения к удаленному компьютеру.
2. Проанализировали скриншоты.
3. Сотрудник переведен на полставки.

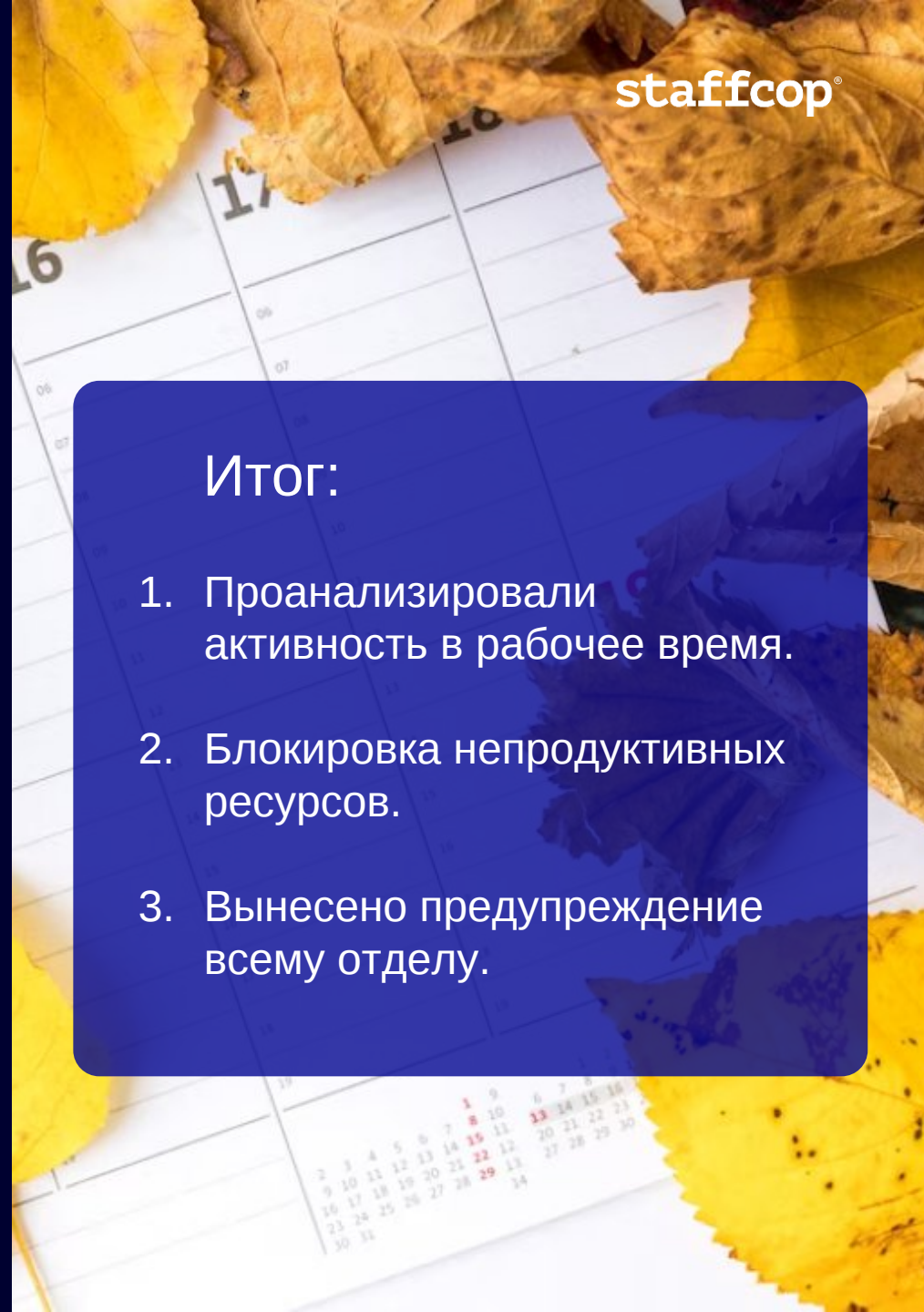
Вот и лето прошло

1. Кто: отдел продаж

1. В августе понизилась активность у целого отдела

1. Не выполнили план месяца из-за того, что занимались подготовкой детей к школе.

1. Компания недополучила прибыль



Итог:

1. Проанализировали активность в рабочее время.
2. Блокировка непродуктивных ресурсов.
3. Вынесено предупреждение всему отделу.

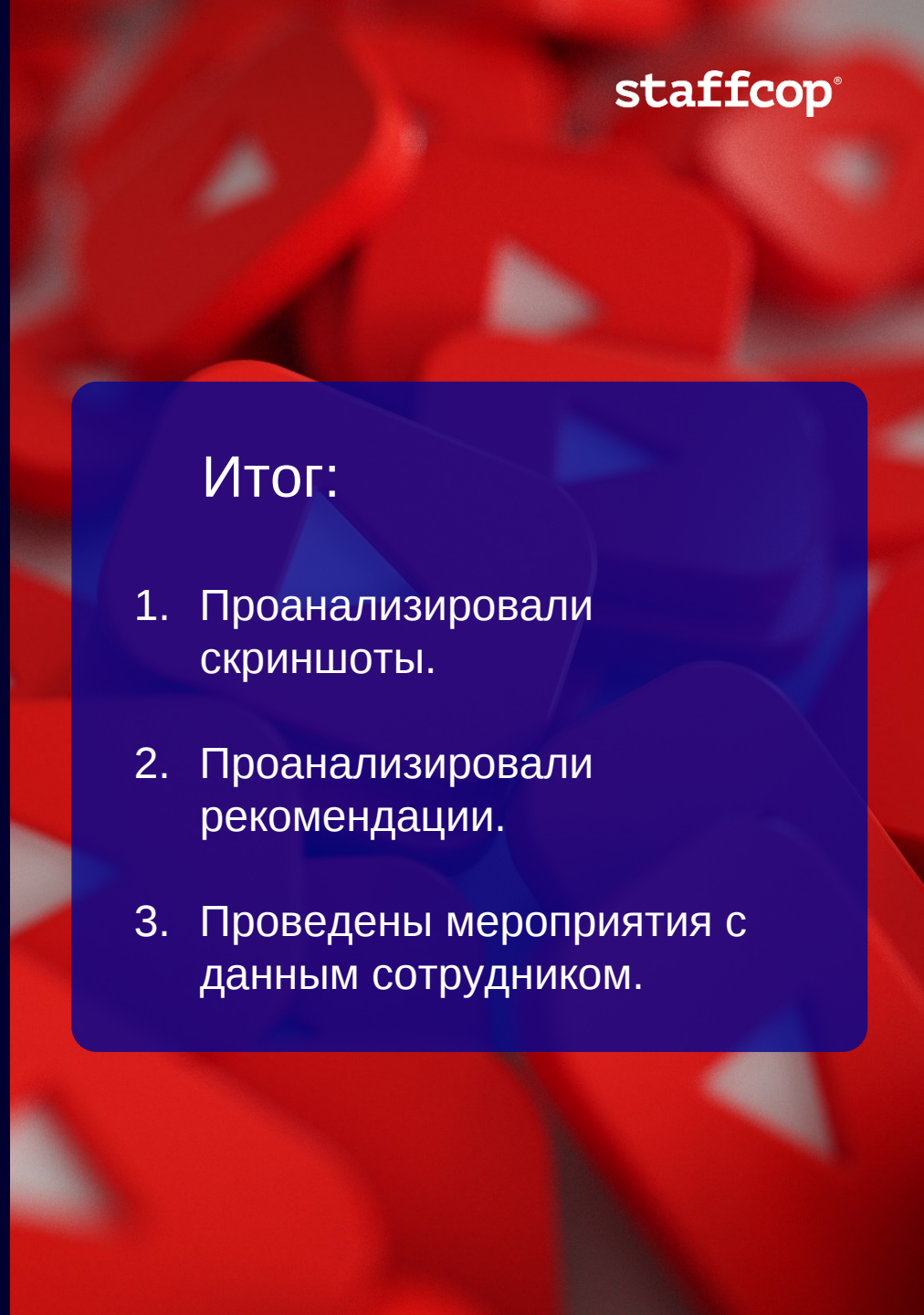
Ябеда Youtube

1. Кто: сотрудник предприятия с КИИ

1. Сотрудник зашел под своим аккаунтом на Youtube

1. В рабочее время смотрел безобидный ролик на Youtube.

1. В рекомендациях обнаружили ролики антироссийской тематики.



Итог:

1. Проанализировали скриншоты.
2. Проанализировали рекомендации.
3. Проведены мероприятия с данным сотрудником.

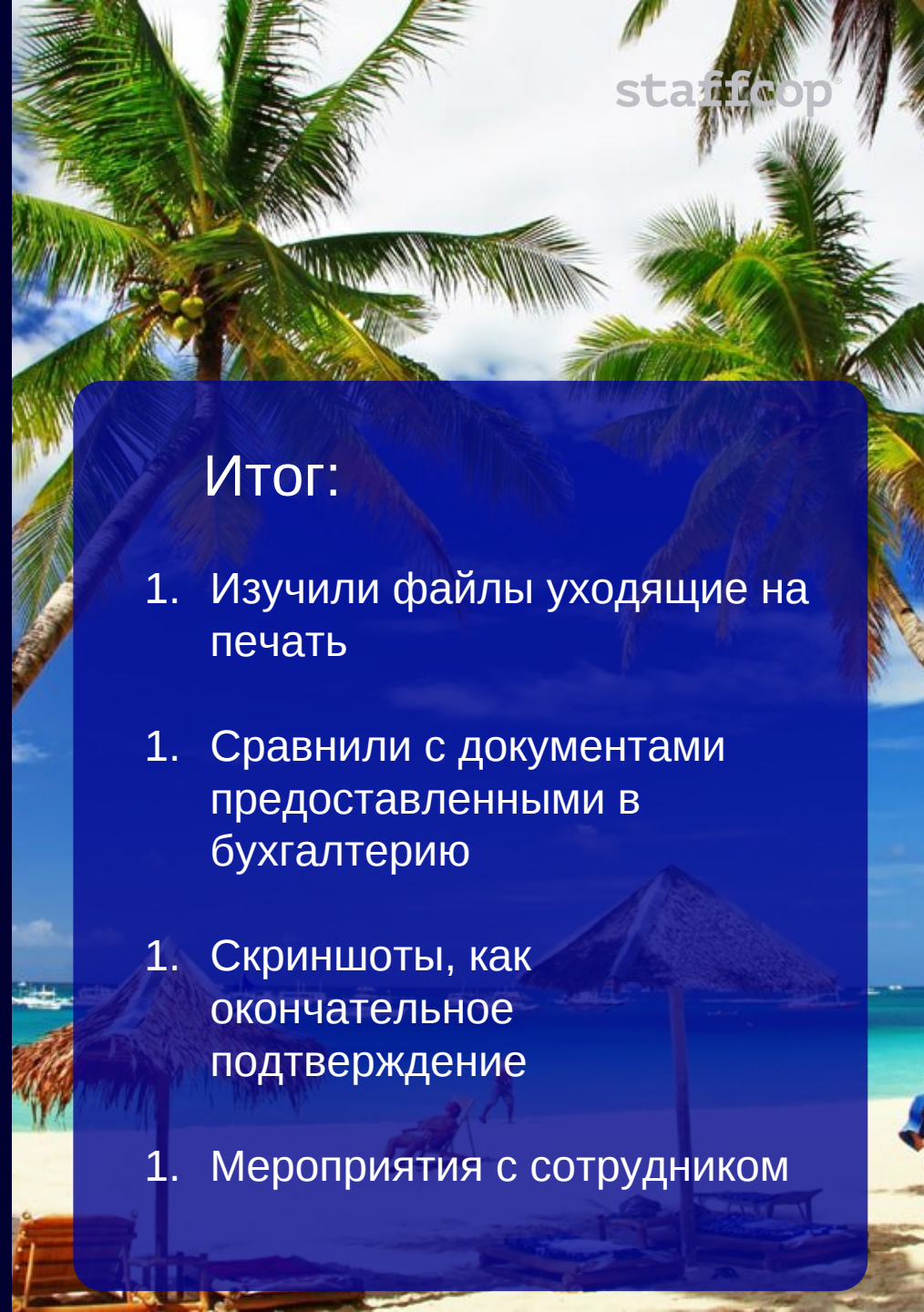
Кейс: Жадный туроператор

1. Работник турфирмы

1. Открывал договор, распечатывал его и принимал деньги от клиентов

1. Не закрывал договор

1. После получения денег исправлял сумму и сохранял новый договор



Итог:

1. Изучили файлы уходящие на печать

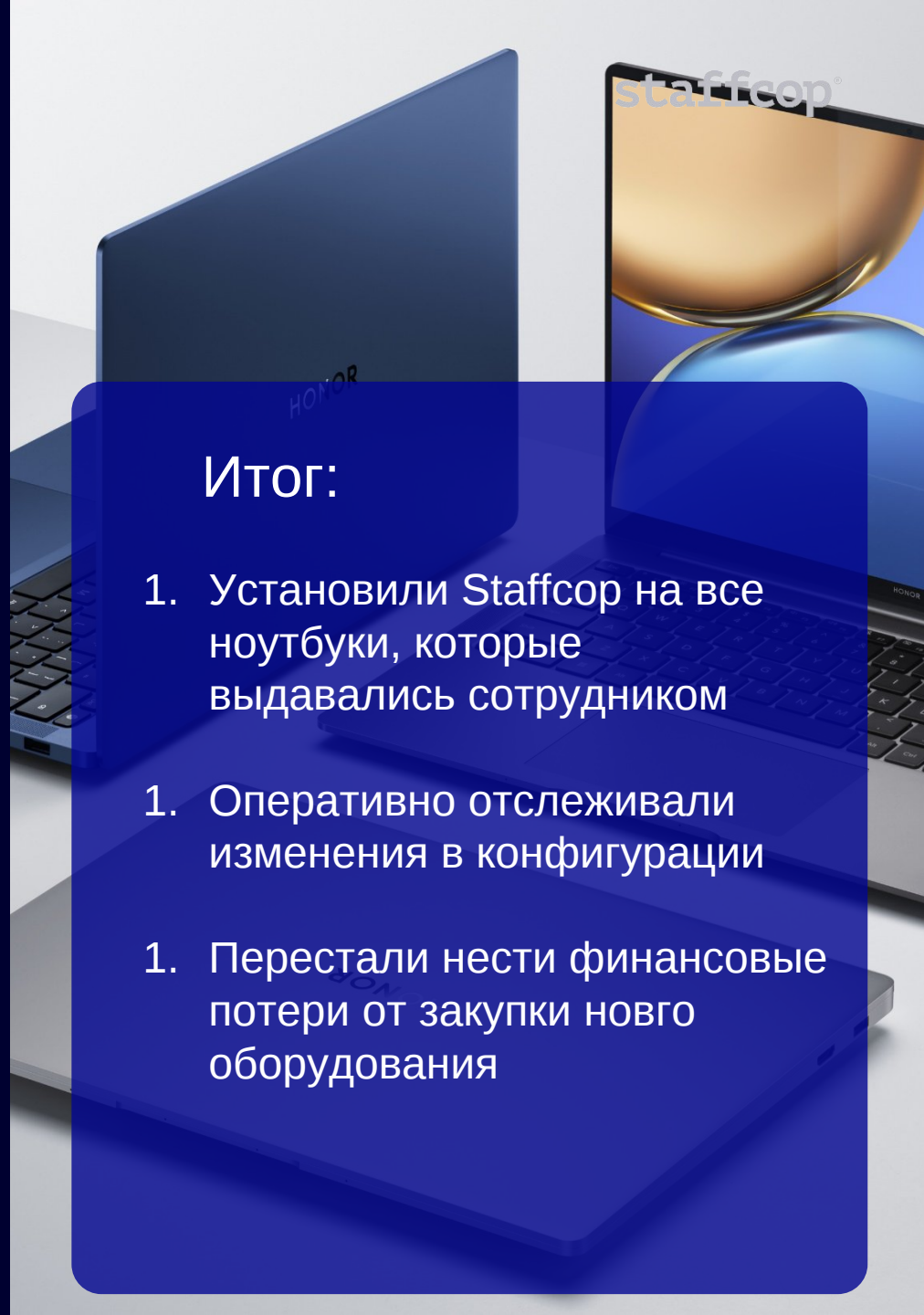
1. Сравнили с документами предоставленными в бухгалтерию

1. Скриншоты, как окончательное подтверждение

1. Мероприятия с сотрудником

Невозвращенцы

1. Увольняемые сотрудники
1. Работали «в полях» на ноутбуках компании
1. При увольнении возвращали ноутбуки
1. Возвращали в неполной комплектации

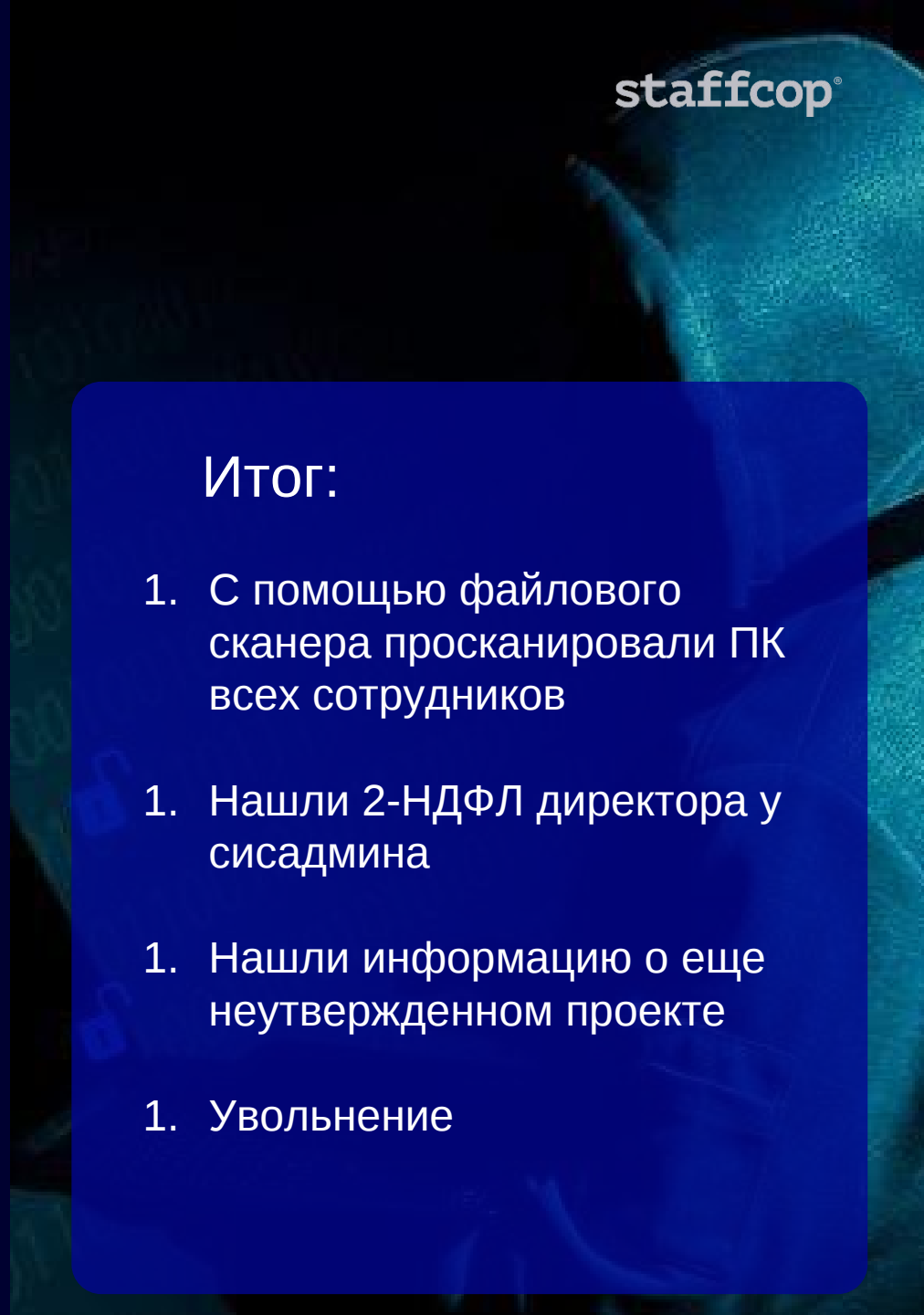


Итог:

1. Установили Staffcop на все ноутбуки, которые выдавались сотрудником
1. Оперативно отслеживали изменения в конфигурации
1. Перестали нести финансовые потери от закупки новго оборудования

Любопытный сисадмин

1. Системный администратор
1. Исследовал файлы на компьютерах руководства
1. Сохранял себе документы
1. Распространял конфиденциальную информацию по компании

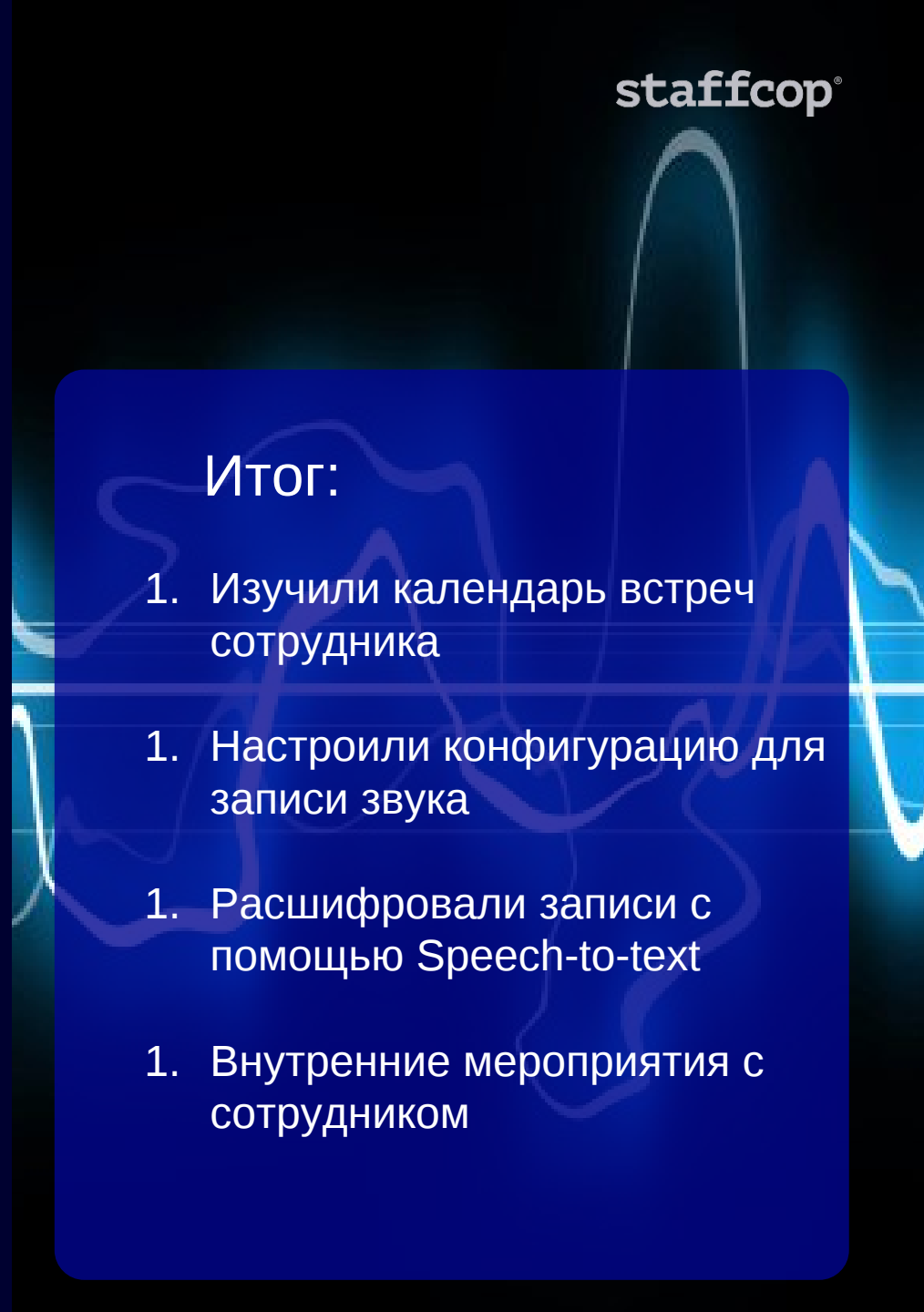


Итог:

1. С помощью файлового сканера просканировали ПК всех сотрудников
1. Нашли 2-НДФЛ директора у сисадмина
1. Нашли информацию о еще неутвержденном проекте
1. Увольнение

Любитель откатов

1. Сотрудник фирмы
1. Часто ездил на личные встречи с заказчиками
1. Брал с собой ноутбук
1. Тет-а-тет договаривался об «откатах»



Итог:

1. Изучили календарь встреч сотрудника
1. Настроили конфигурацию для записи звука
1. Расшифровали записи с помощью Speech-to-text
1. Внутренние мероприятия с сотрудником

Преимущества Staffcop Enterprise

staffcop®

- Кроссплатформенный
- Быстрый и легкий
- Простое и доступное лицензирование
- Импортонезависимый
- Качественная техническая поддержка
- Индивидуальный подход, закрепленный менеджер
- Расширенный пилот с полноценным функционалом
- Доступ к регулярным обновлениям

Если у вас уже есть DLP решения

staffcop

Эшелонированная защита

На одной группе риска DLP.
На другой - Staffcop

DLP на шлюзе.
Staffcop на end point

Оптимизируйте бюджет защиты ИБ

Тестируйте Staffcop бесплатно !

Быстро

Развертывание пилотного проекта обычно занимает не более одного дня

Легко

Требуется минимум усилий и ресурсов для запуска

Комплексно

Вы сможете оценить сразу весь комплекс решаемых задач и принять правильное решение

Полное техническое сопровождение на этапе тестирования!

Спасибо за внимание!

«Безопасность — это не продукт и не результат, это процесс» */ Брюс Шнайер /*

Станислав Юдинских

Менеджер проектного офиса
ООО Атом Безопасность
s.yudinskikh@staffcop.ru

staffcop.ru

telegram