staffcop®

Расследование инцидентов
внутренней безопасности

Внутренние угрозы: Истории и расследования

Станислав Юдинских

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

staffcop®

> 66 %

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

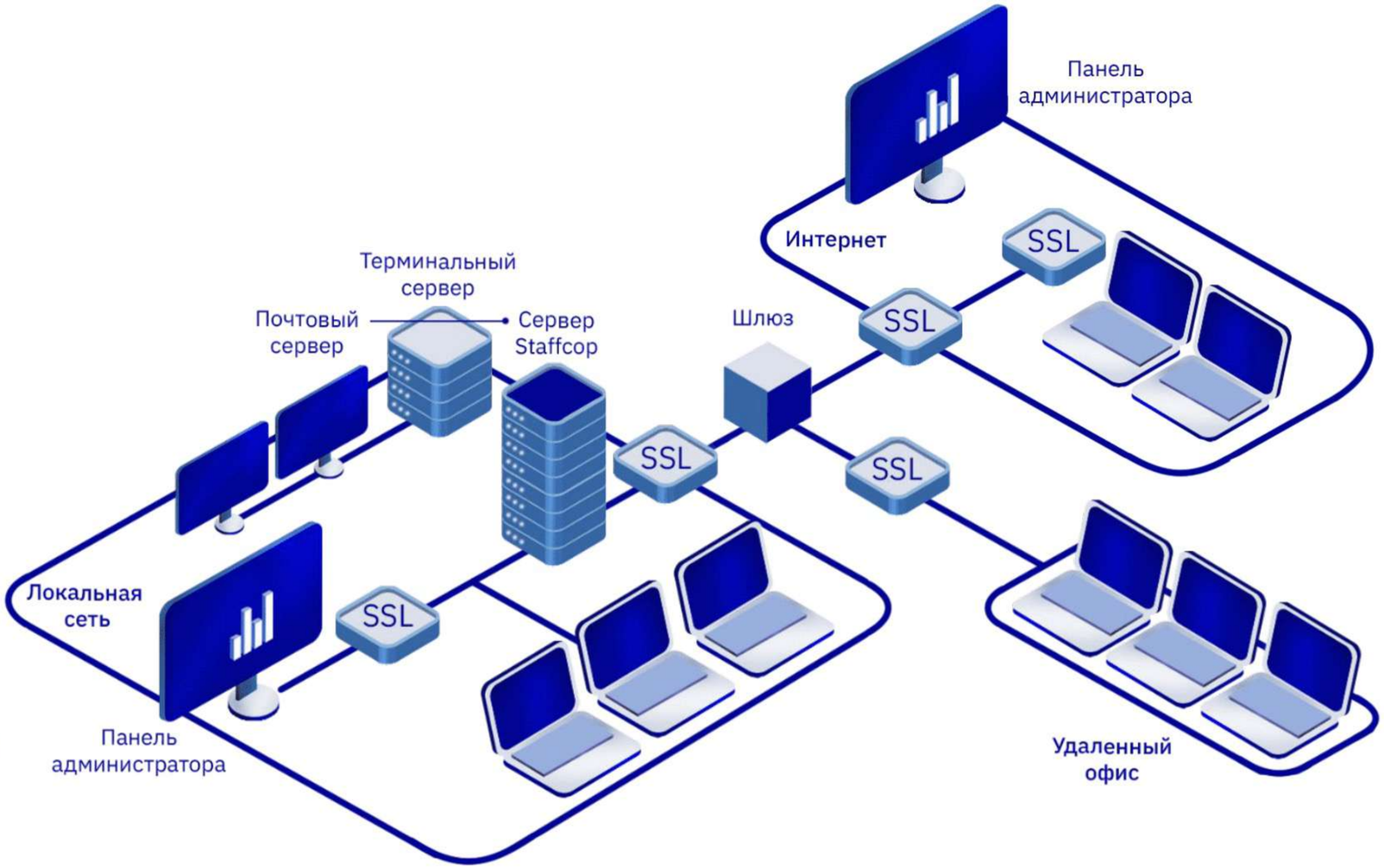
IT специалистов

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

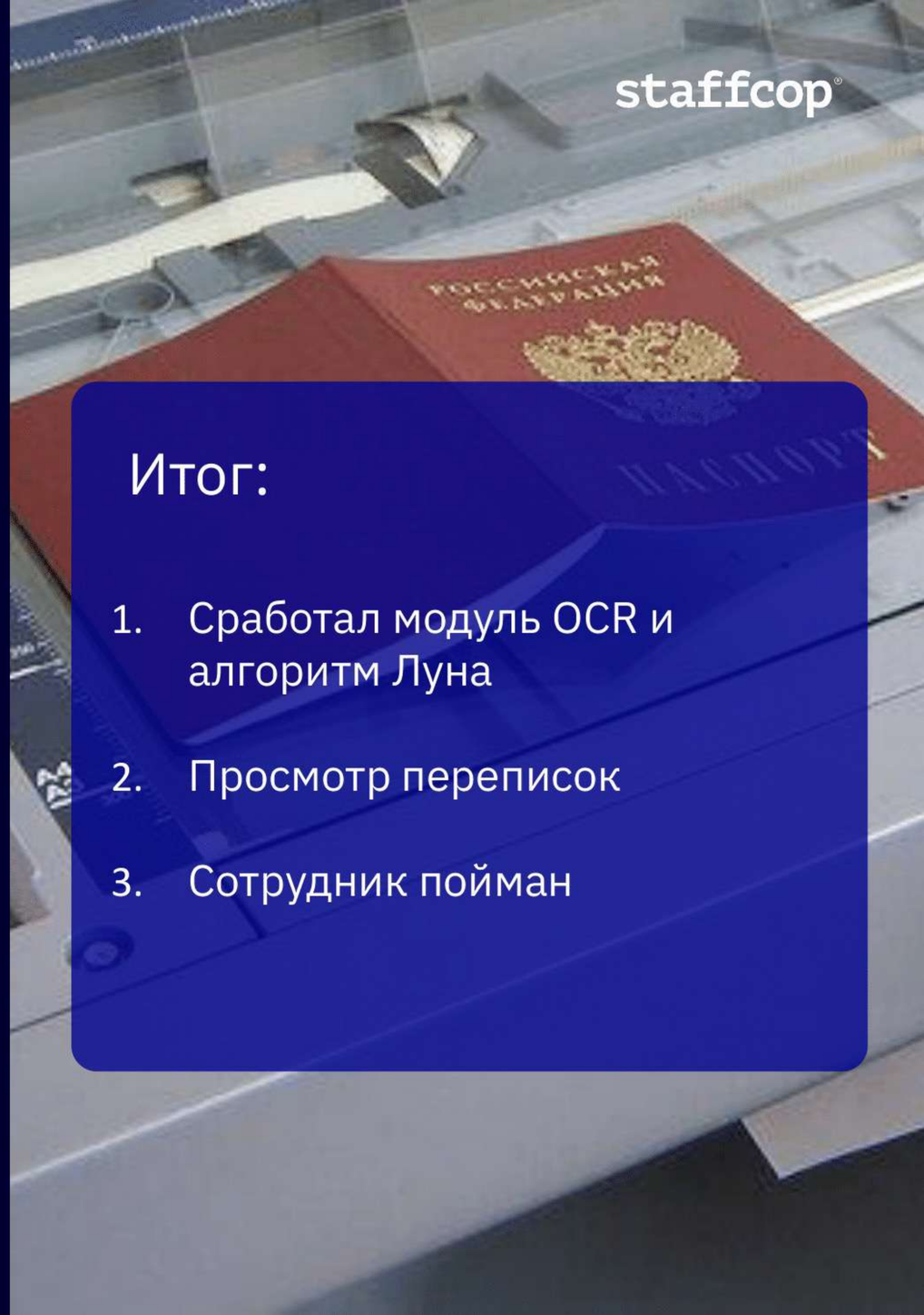
staffcop

Кейсы

Пять случаев на мониторе: уроки из мира кибербезопасности

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

1. Кто: Сотрудница банка
2. Отправила с личной почты и через мессенджеры сканы паспорта и номер карты клиента
3. Пыталась передать третьему лицу для мошеннических действий
4. Что грозило компании: репутационные риски и нарушение предписаний регуляторов, штрафы



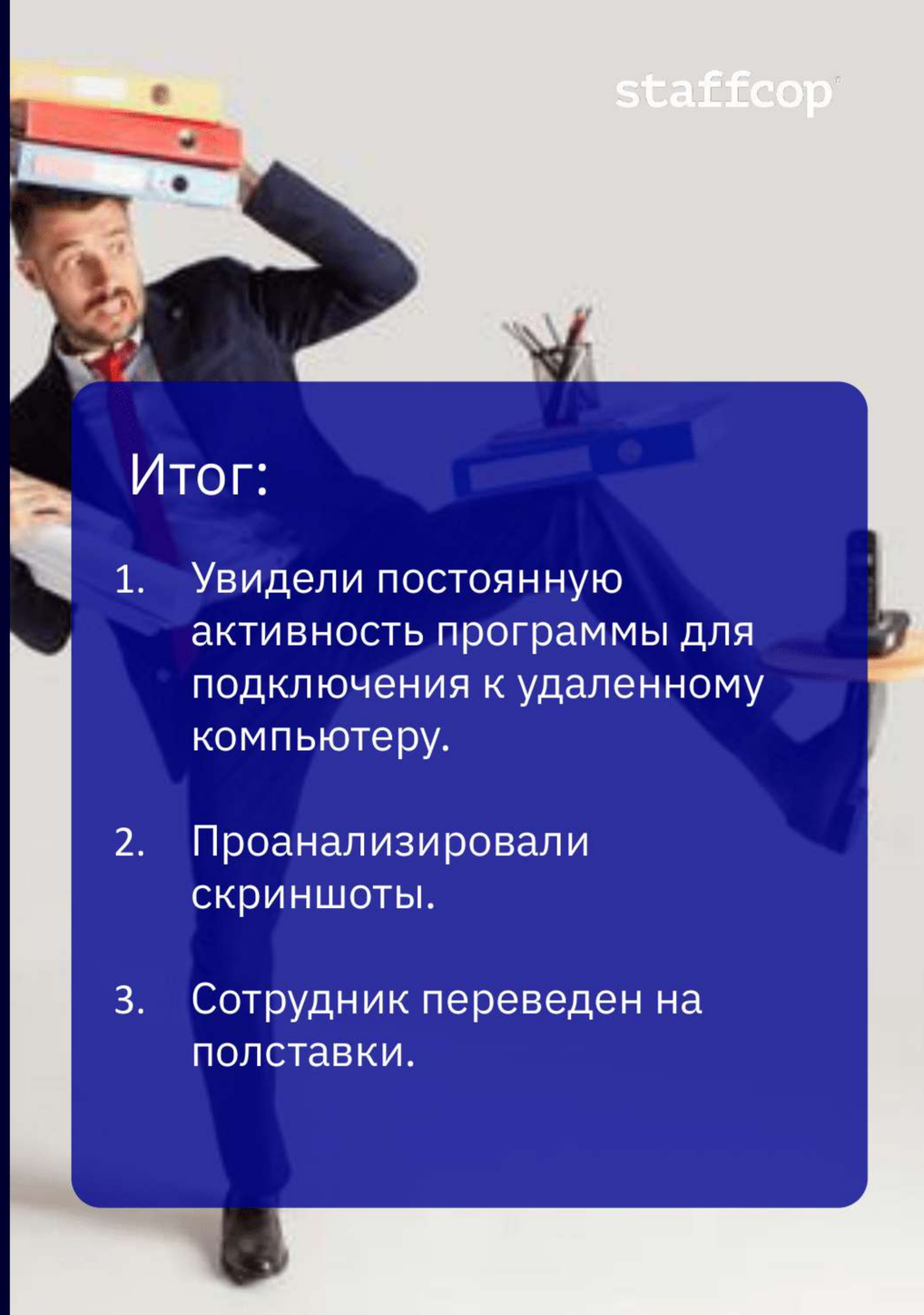
staffcop

Итог:

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

Параллельный бизнес

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

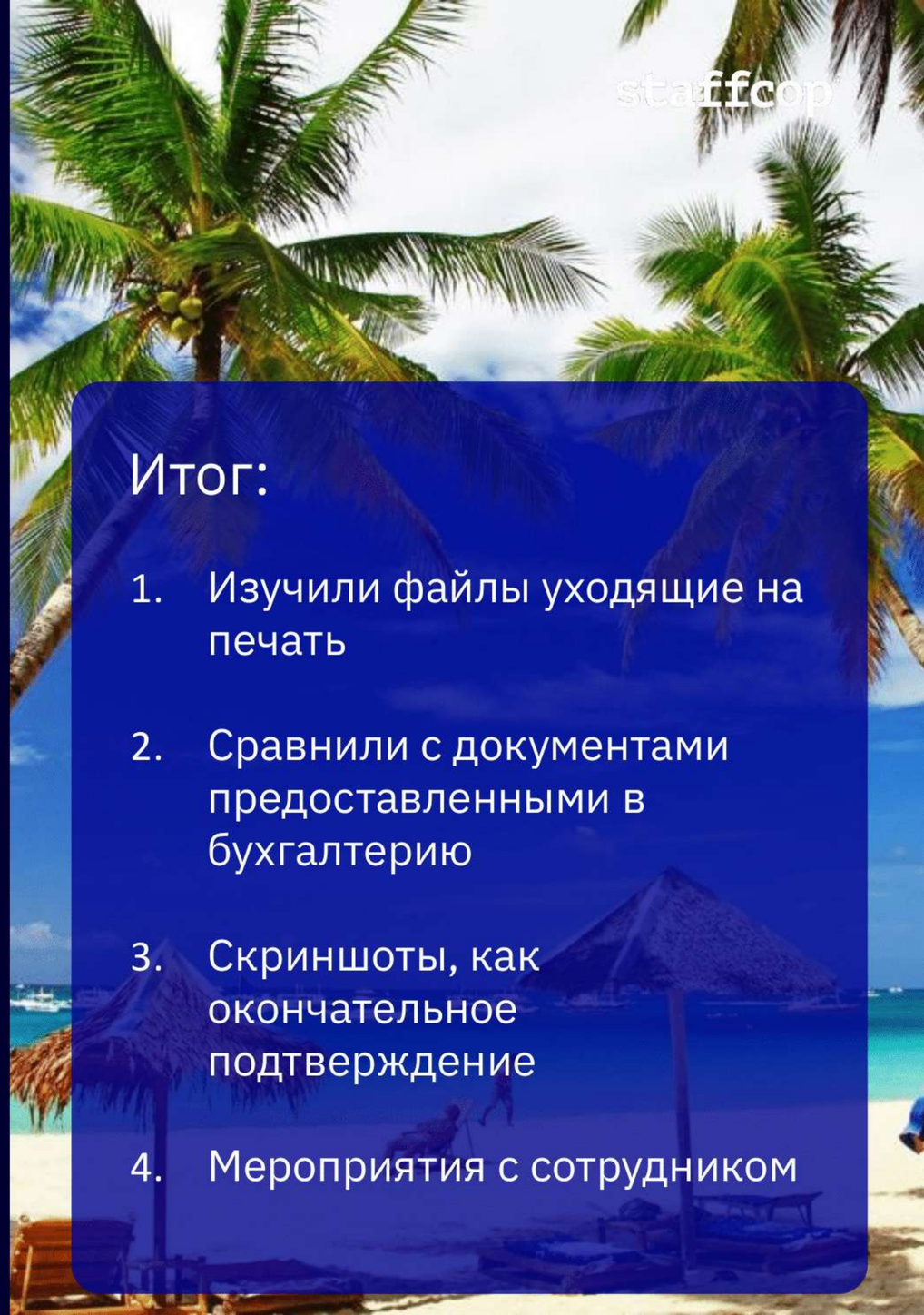


Итог:

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

Кейс: Жадный туроператор

1. Работник турфирмы
2. Открывал договор, распечатывал его и принимал деньги от клиентов
3. Не закрывал договор
4. После получения денег исправлял сумму и сохранял новый договор

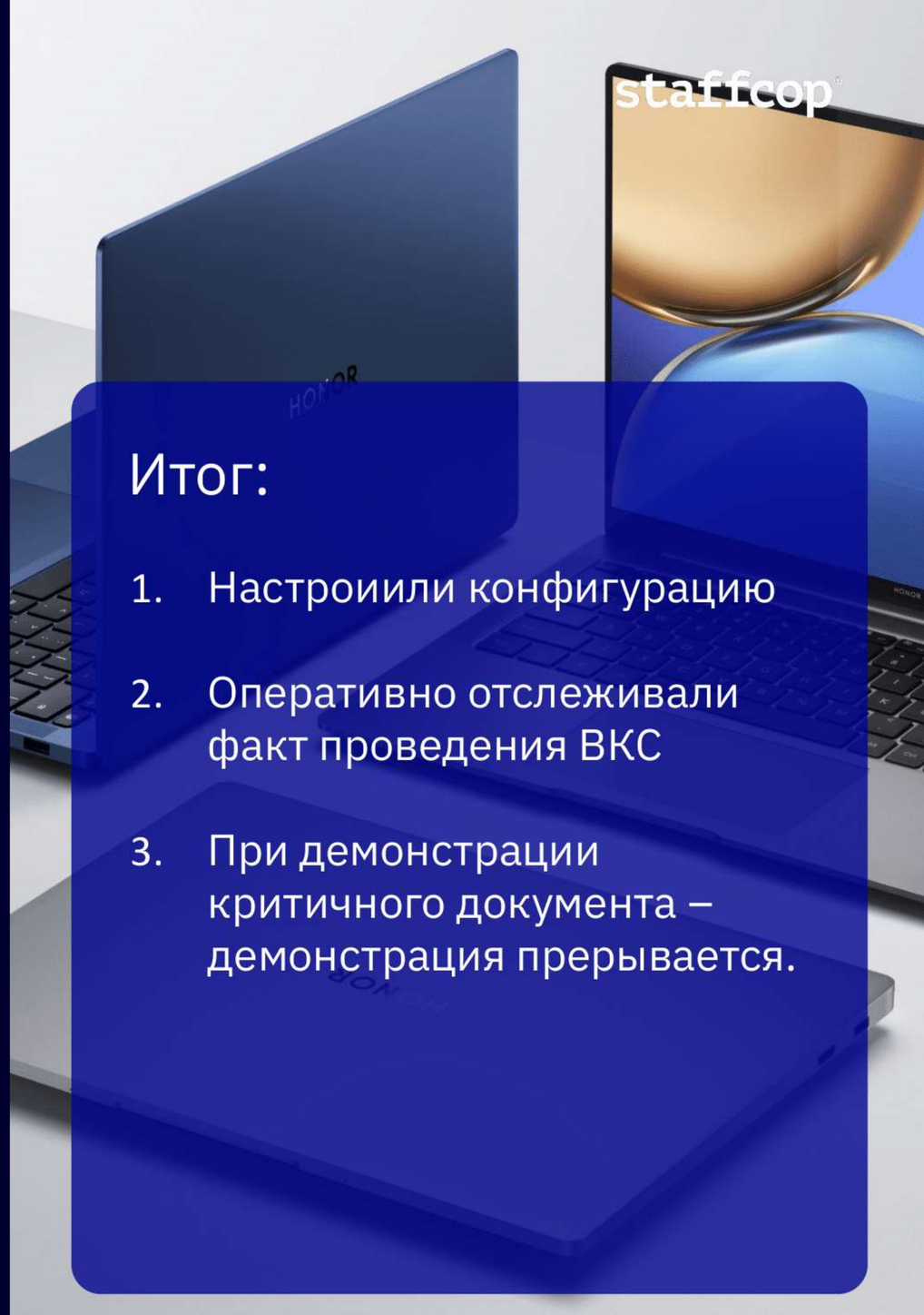


Итог:

1. Изучили файлы уходящие на печать
2. Сравнили с документами предоставленными в бухгалтерию
3. Скриншоты, как окончательное подтверждение
4. Мероприятия с сотрудником

Утечка через ВКС

1. Сотрудник демонстрировал критичные документы через ВКС
2. На «той» стороне производилась запись
3. Компания теряла деньги

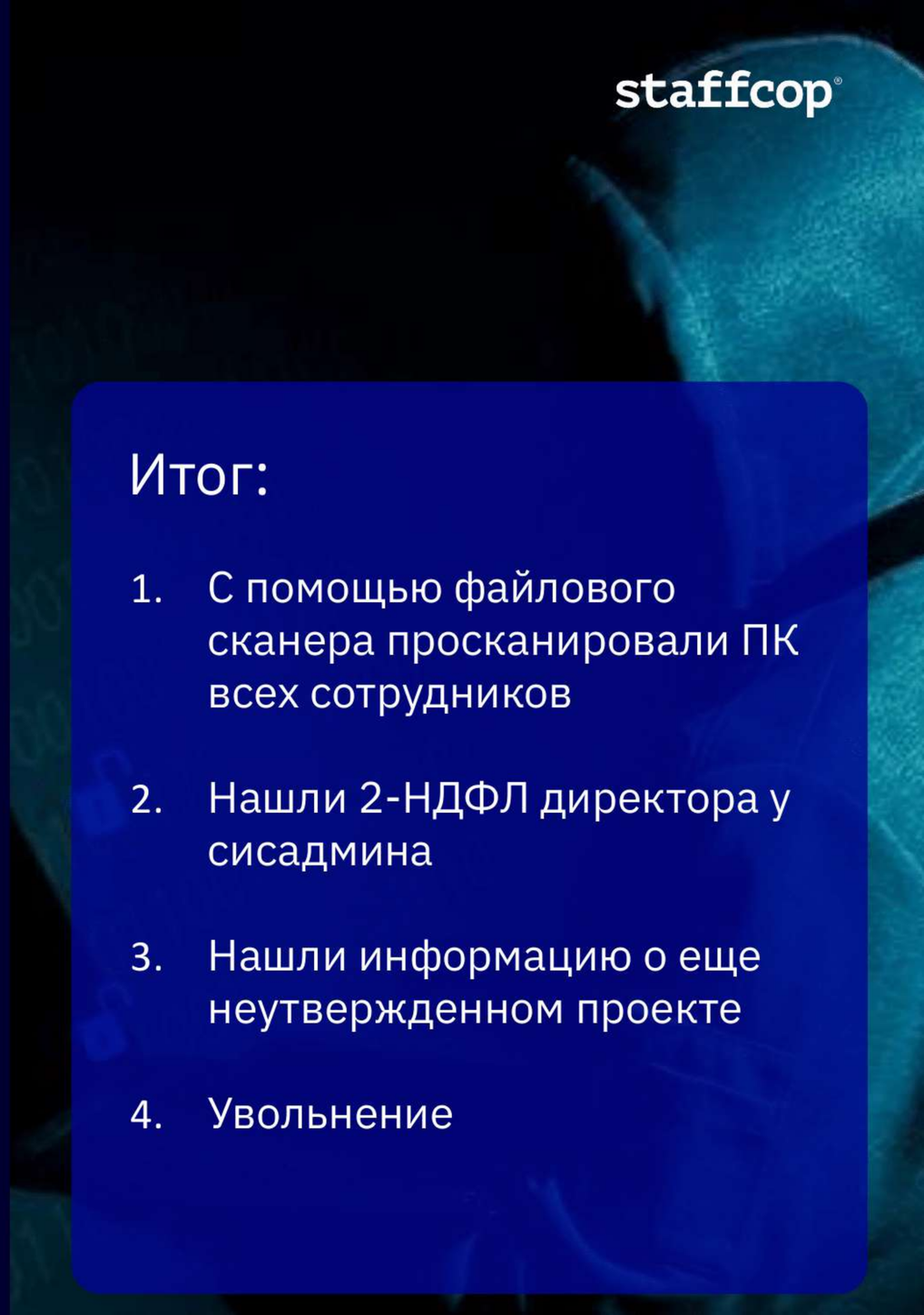


Итог:

1. Настроиили конфигурацию
2. Оперативно отслеживали факт проведения ВКС
3. При демонстрации критичного документа – демонстрация прерывается.

Любопытный сисадмин

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



Итог:

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

Люди как угроза

staffcop

- Количество будет расти
- Атаки будут усложняться
- Утечки через шантаж
- Утечки через глупость

«Безопасность — это не продукт и не результат, это процесс»

/ Брюс Шнайер /

Спасибо за внимание!

Станислав Юдинских

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

staffcop.ru

Telegram