staffcop®

Расследование инцидентов и контроль информационных потоков

Янушко Сергей

Старший менеджер отдела по работе
с партнерами ООО «АТОМ БЕЗОПАСНОСТЬ»

«Любая система небезопасна»

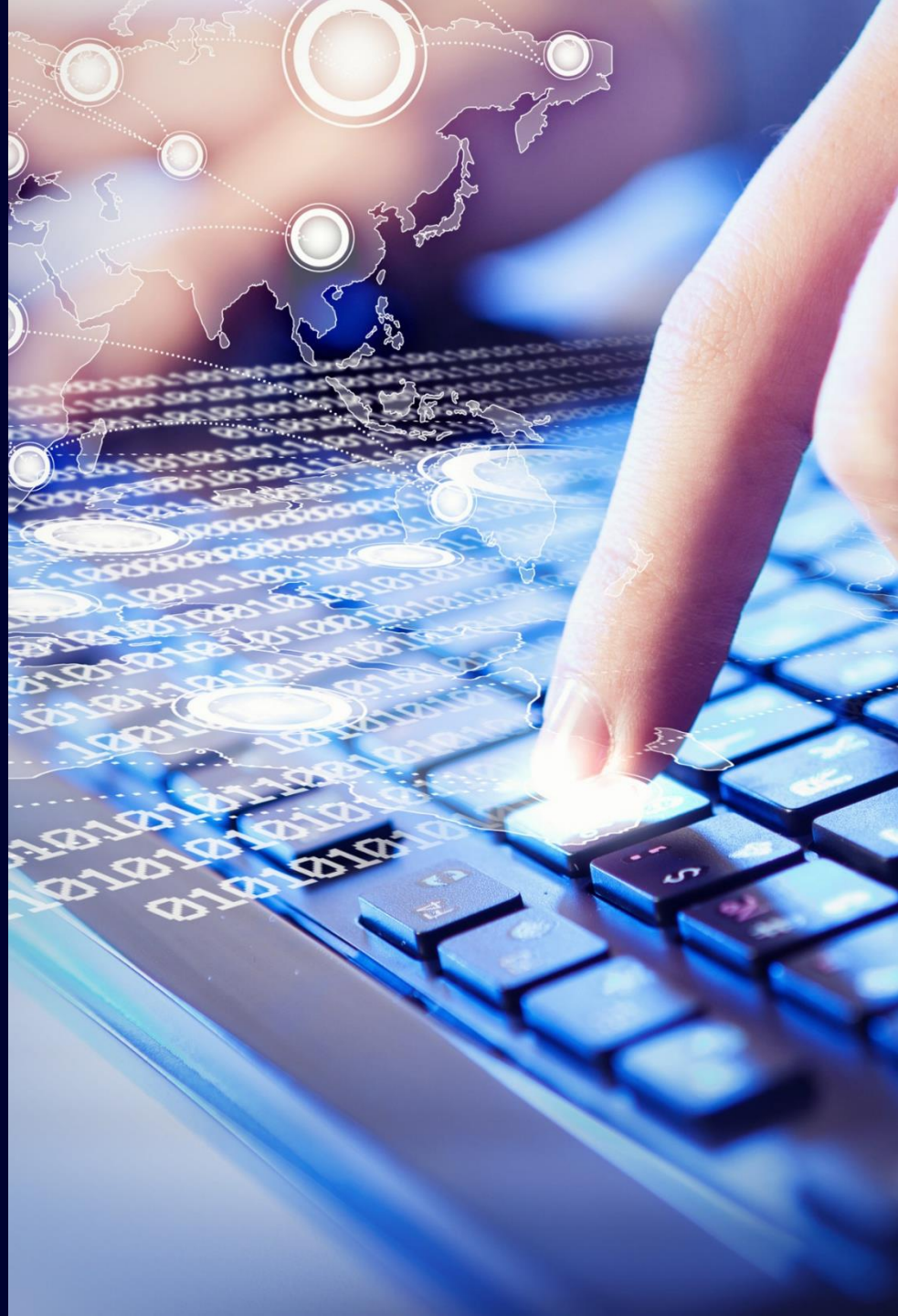
100% защиты не бывает!

staffcop®

Слив будет всегда!

- Человеческий фактор
- Программная уязвимость
- Хакерская атака

2/3 атак – изнутри!
Статистика от Staffcop



staffcop®

Кто виноват?

Давайте разберемся!

staffcop®

Инструменты для разбирательства

Действия пользователей

- Снимки с web камеры
- **Скриншоты и запись видео с рабочего стола**
- Мониторинг посещенных сайтов
- **Контроль печати**
- Мониторинг действий в социальных сетях
- **Запись аудио с микрофона и колонок**

Документы и файлы

- Контроль почты
- **Перехват мессенджеров**
- Мониторинг доступа к файлам

Действия системы

- Удаленное управление
- **Контроль съемных носителей**
- Инвентаризация ПО

staffcop®

Чем поможем?

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

staffcop®

Кому поможем?

Собственников бизнеса

IT специалистов

ИБ специалистов

Сотрудников HR

Собственникам бизнеса

IT специалистам

Сотрудникам HR

ИБ специалистам

Аналитические возможности

01 Архив данных

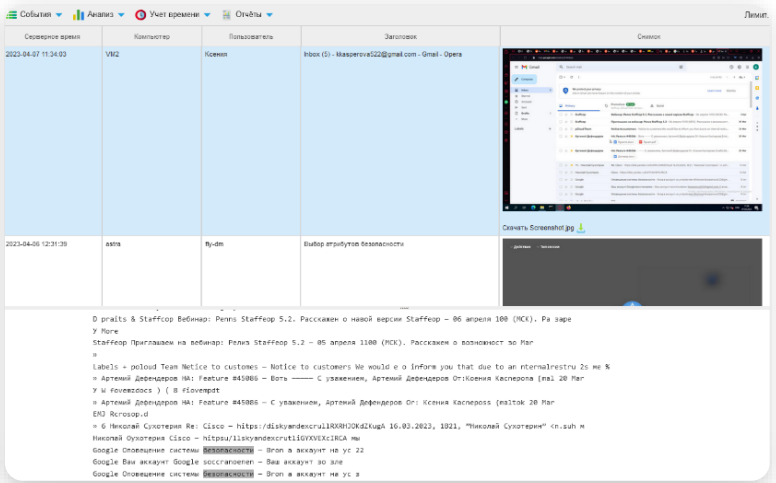
02 Поиск по словам и регулярным выражениям

03 Синхронизация данных с AD

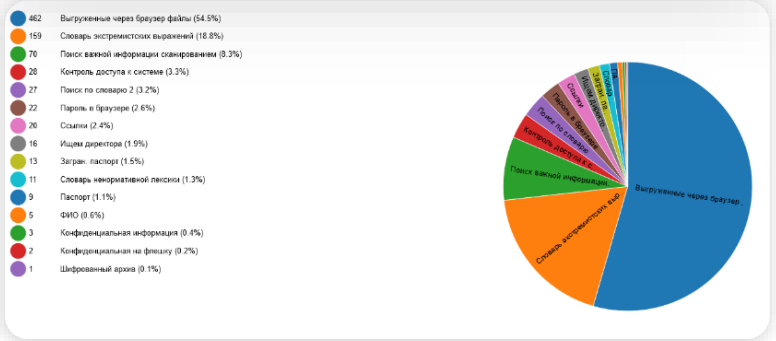
04 Конструктор многомерных отчетов

05 Множество графов и диаграмм

06 Speech-to-text



Astra Воронеж	Вход/выход из системы	6
Astra Воронеж	Буфер обмена	47
Astra Воронеж	Устройства	67
Astra Воронеж	Внешние диски	16
Astra Воронеж	Операции с файлами	41289
Astra Воронеж	Реестр оборудования	1001
Astra Воронеж	Реестр софта	8660
Astra Воронеж	Поисковый запрос	15
Astra Воронеж	Видео рабочего стола	7
Astra Воронеж	Терминал linux	4
Astra Воронеж	Линукс лог	7
Astra Воронеж	Время активности	1343



staffcop®

Собственникам бизнеса

ИБ специалистам

Расследование инцидентов ИБ

01 Система оповещений

02 Гибкая система настройки фильтров

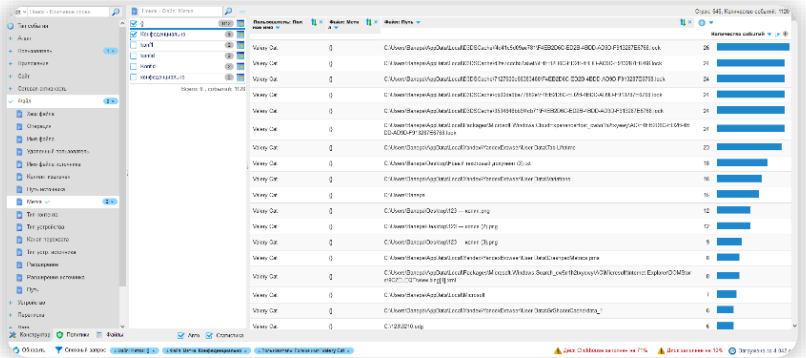
03 Графы взаимосвязей

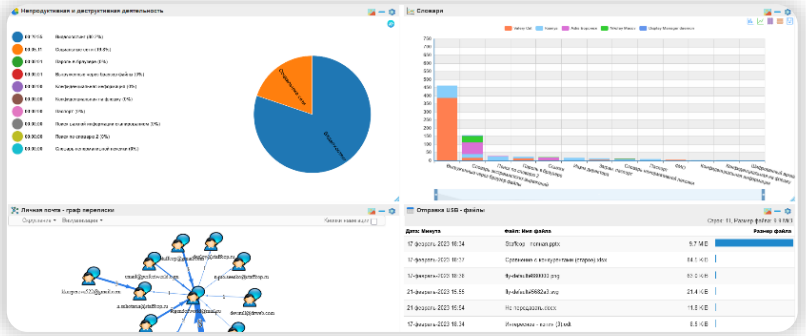
04 Метки для файлов

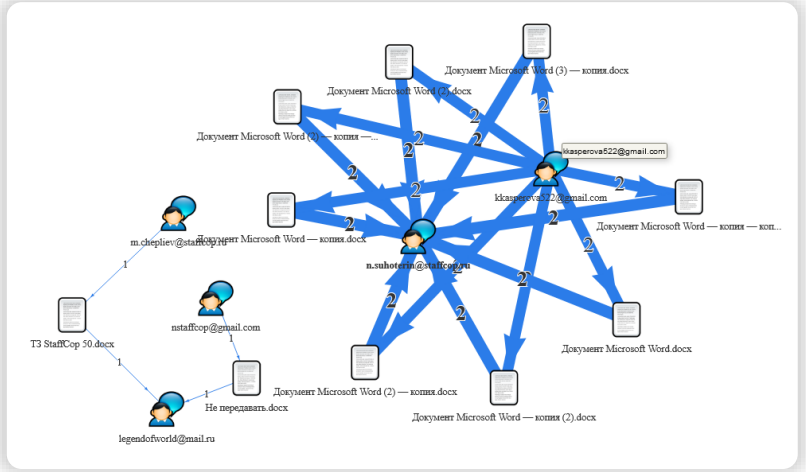
05 Изменение конфигурации контроля при наступлении определённого события

06 Защита от массового копирования

07 Нейронная сеть распознавания изображений







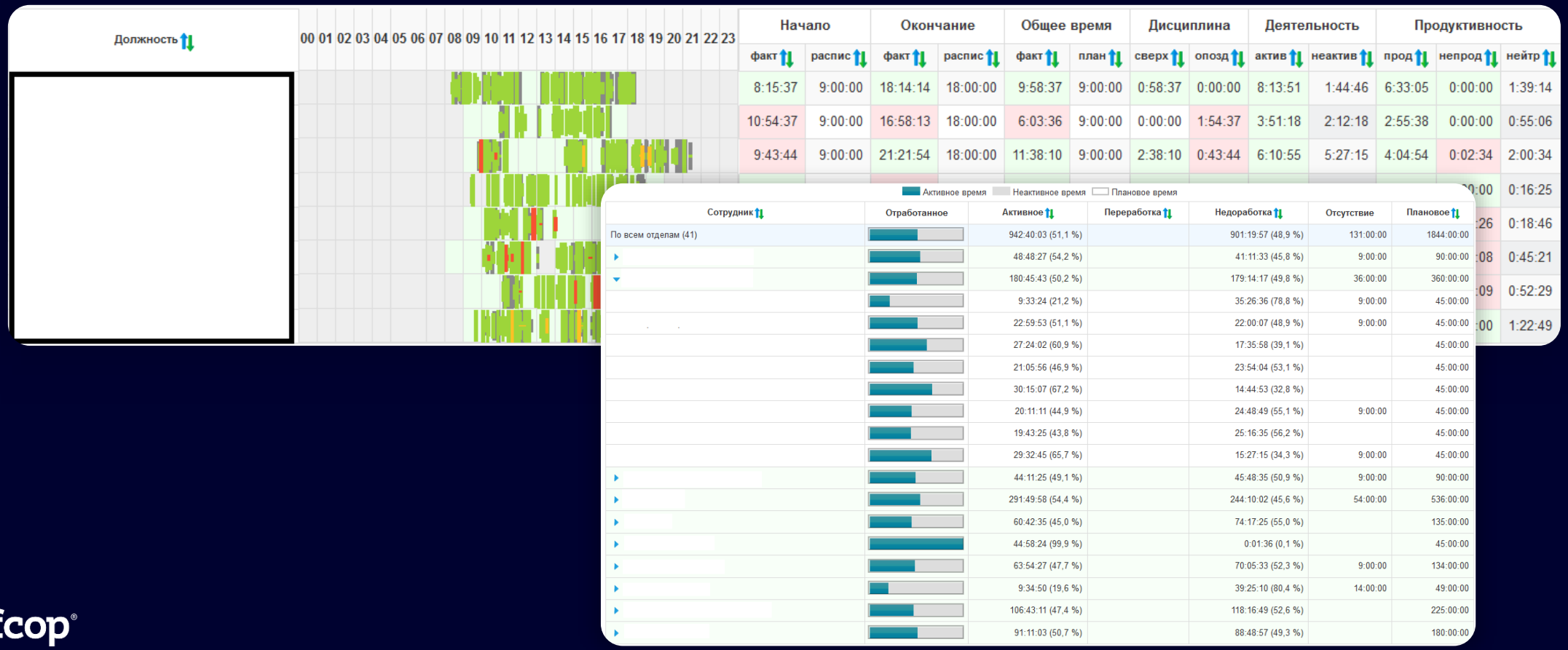
staffcop®

Собственникам бизнеса

Сотрудникам HR

Учет рабочего времени и его оценка

Заняты работой	Личные дела	Опоздания	Простой в работе	Прочее
24%	37%	7%	13%	19%



Должность	00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23	Начало		Окончание		Общее время		Дисциплина		Деятельность		Продуктивность		
		факт	распис	факт	распис	факт	план	сверх	опозд	актив	неактив	прод	непрод	нейтр
		8:15:37	9:00:00	18:14:14	18:00:00	9:58:37	9:00:00	0:58:37	0:00:00	8:13:51	1:44:46	6:33:05	0:00:00	1:39:14
		10:54:37	9:00:00	16:58:13	18:00:00	6:03:36	9:00:00	0:00:00	1:54:37	3:51:18	2:12:18	2:55:38	0:00:00	0:55:06
		9:43:44	9:00:00	21:21:54	18:00:00	11:38:10	9:00:00	2:38:10	0:43:44	6:10:55	5:27:15	4:04:54	0:02:34	2:00:34
														0:16:25
														0:18:46
														0:45:21
														0:52:29
														1:22:49

Активное время | Неактивное время | Плановое время

Сотрудник	Отработанное	Активное	Переработка	Недоработка	Отсутствие	Плановое
По всем отделам (41)		942:40:03 (51,1 %)		901:19:57 (48,9 %)	131:00:00	1844:00:00
		48:48:27 (54,2 %)		41:11:33 (45,8 %)	9:00:00	90:00:00
		180:45:43 (50,2 %)		179:14:17 (49,8 %)	36:00:00	360:00:00
		9:33:24 (21,2 %)		35:26:36 (78,8 %)	9:00:00	45:00:00
		22:59:53 (51,1 %)		22:00:07 (48,9 %)	9:00:00	45:00:00
		27:24:02 (60,9 %)		17:35:58 (39,1 %)		45:00:00
		21:05:56 (46,9 %)		23:54:04 (53,1 %)		45:00:00
		30:15:07 (67,2 %)		14:44:53 (32,8 %)		45:00:00
		20:11:11 (44,9 %)		24:48:49 (55,1 %)	9:00:00	45:00:00
		19:43:25 (43,8 %)		25:16:35 (56,2 %)		45:00:00
		29:32:45 (65,7 %)		15:27:15 (34,3 %)	9:00:00	45:00:00
		44:11:25 (49,1 %)		45:48:35 (50,9 %)	9:00:00	90:00:00
		291:49:58 (54,4 %)		244:10:02 (45,6 %)	54:00:00	536:00:00
		60:42:35 (45,0 %)		74:17:25 (55,0 %)		135:00:00
		44:58:24 (99,9 %)		0:01:36 (0,1 %)		45:00:00
		63:54:27 (47,7 %)		70:05:33 (52,3 %)	9:00:00	134:00:00
		9:34:50 (19,6 %)		39:25:10 (80,4 %)	14:00:00	49:00:00
		106:43:11 (47,4 %)		118:16:49 (52,6 %)		225:00:00
		91:11:03 (50,7 %)		88:48:57 (49,3 %)		180:00:00

staffcop®

IT специалистам

ИБ специалистам

Администрирование

01 Мониторинг аномальной активности

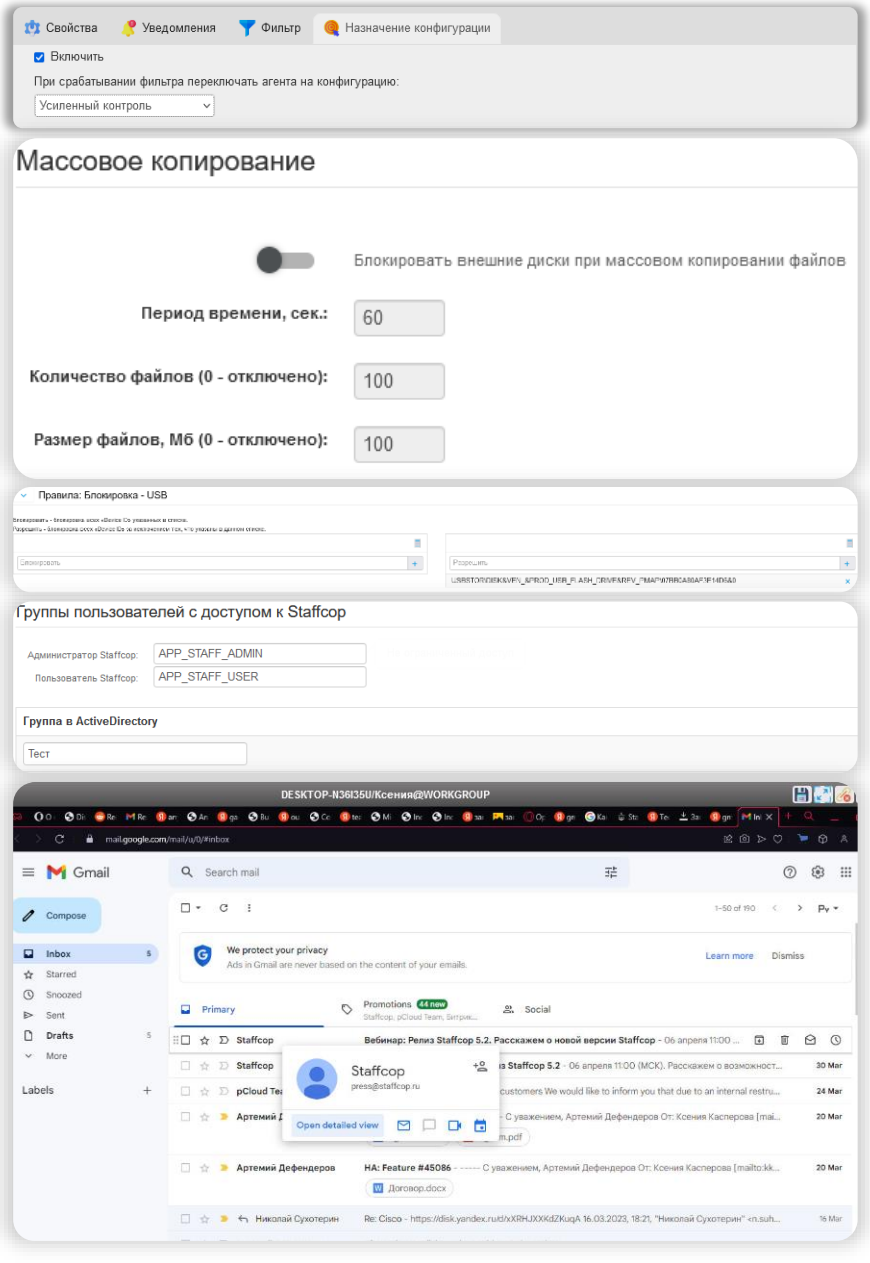
02 Блокировки съемных носителей

03 Инвентаризация ПО и «железа»

04 Удаленное наблюдение за АРМ и перехват управления

05 Интеграция с SIEM, AD, 1С, СКУД и другими системами ИБ и ИТ

06 Разные доступы для разных пользователей системы



staffcop®

Расследование инцидентов. Сбор доказательной базы

Утечка информации.
Потеря данных

Риски, связанные с
удаленной работой

Дисциплина сотрудников

Предупреждение опасных
действий и мошеннических схем
сотрудников

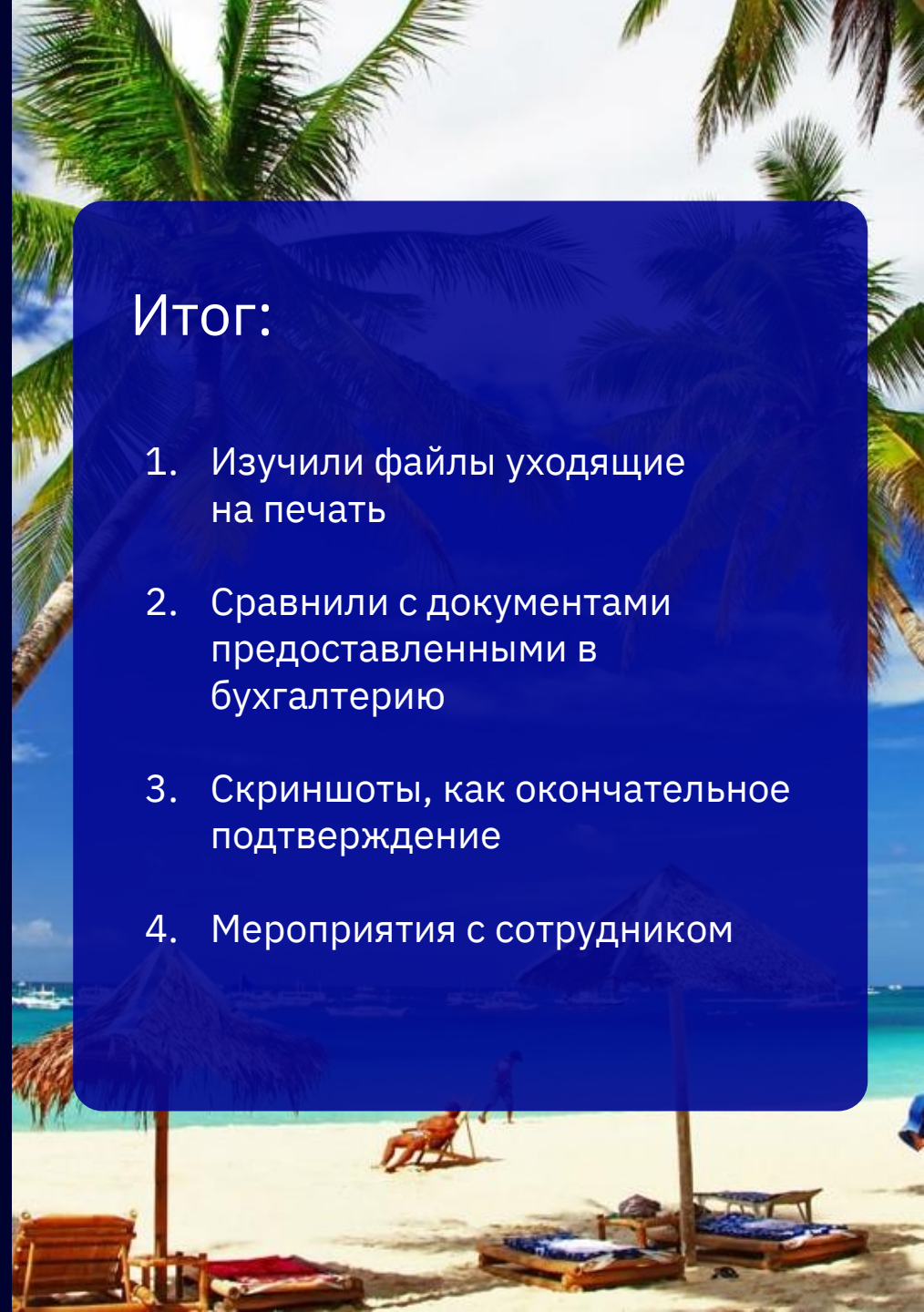
Контроль периферийного
оборудования и ПО

Возможность сбора
доказательной базы

staffcop®

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



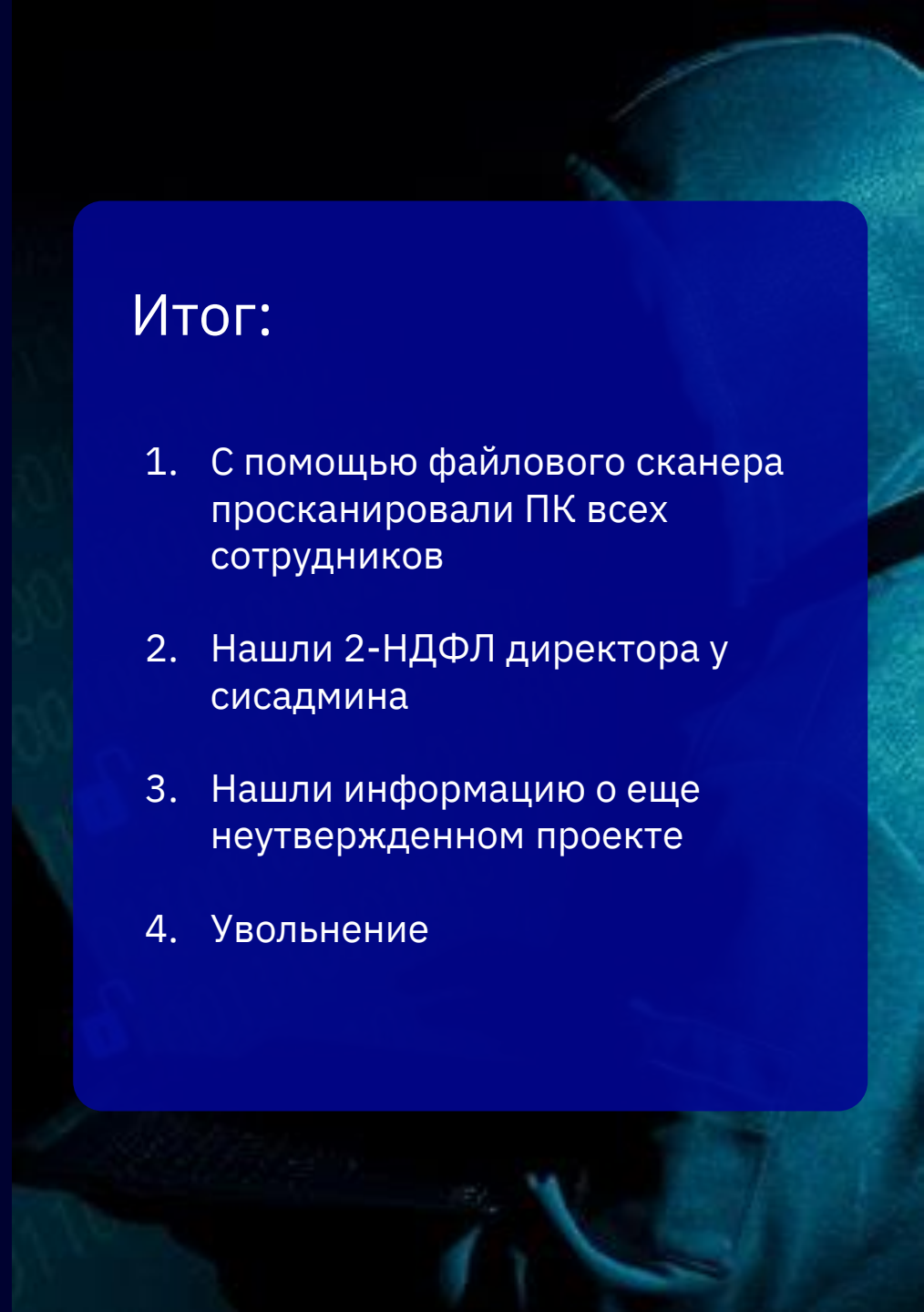
Итог:

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

staffcop®

Кейс: Любопытный сисадмин

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

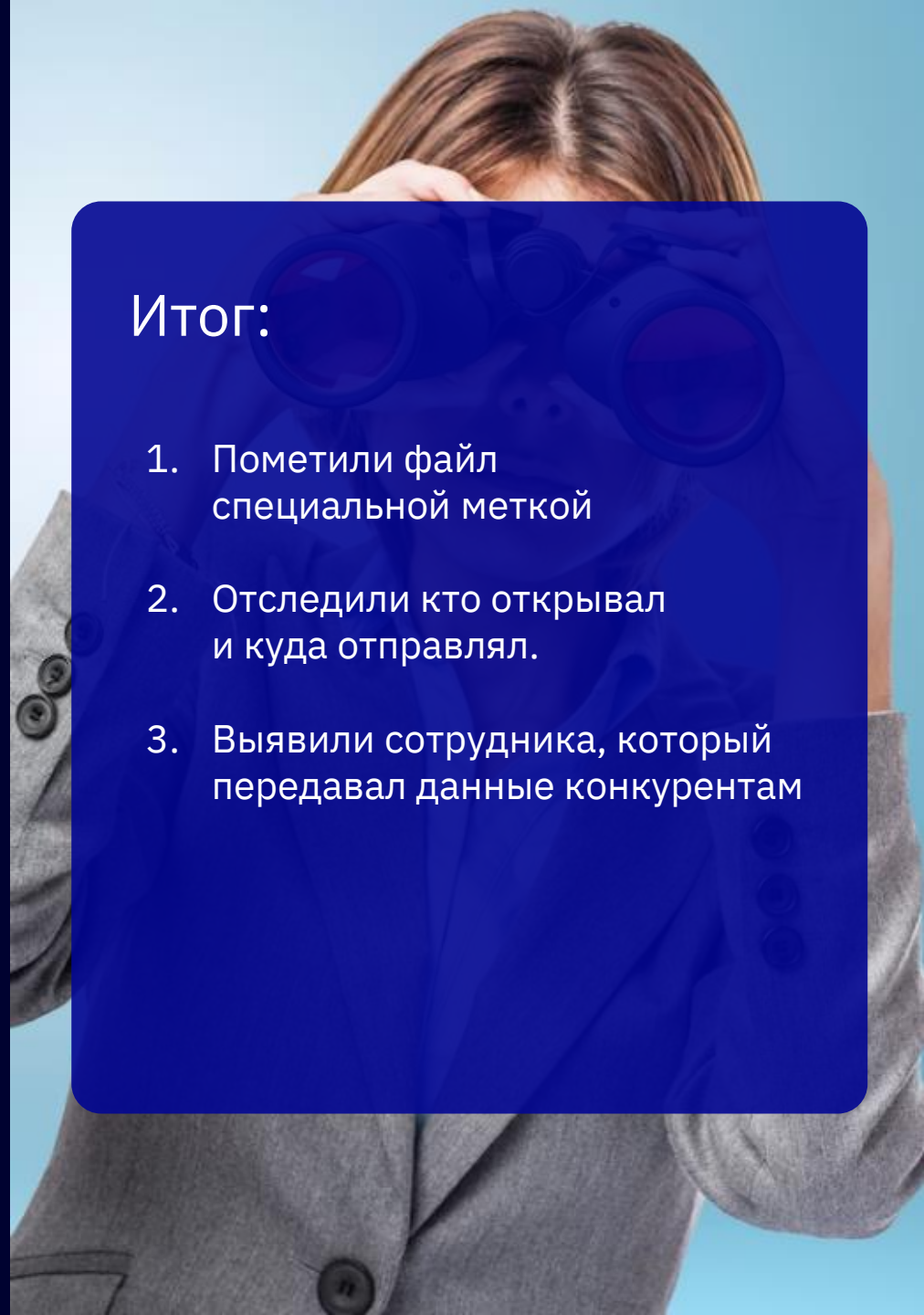


Итог:

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

Кейс: Работа на конкурентов

1. Кто: Менеджер по продажам
2. Фирма по производству пластиковых окон заметила, что конкуренты быстрее реагируют на заявки
3. Сотрудник «сливал» заявки конкурентам
4. Значительный финансовый ущерб



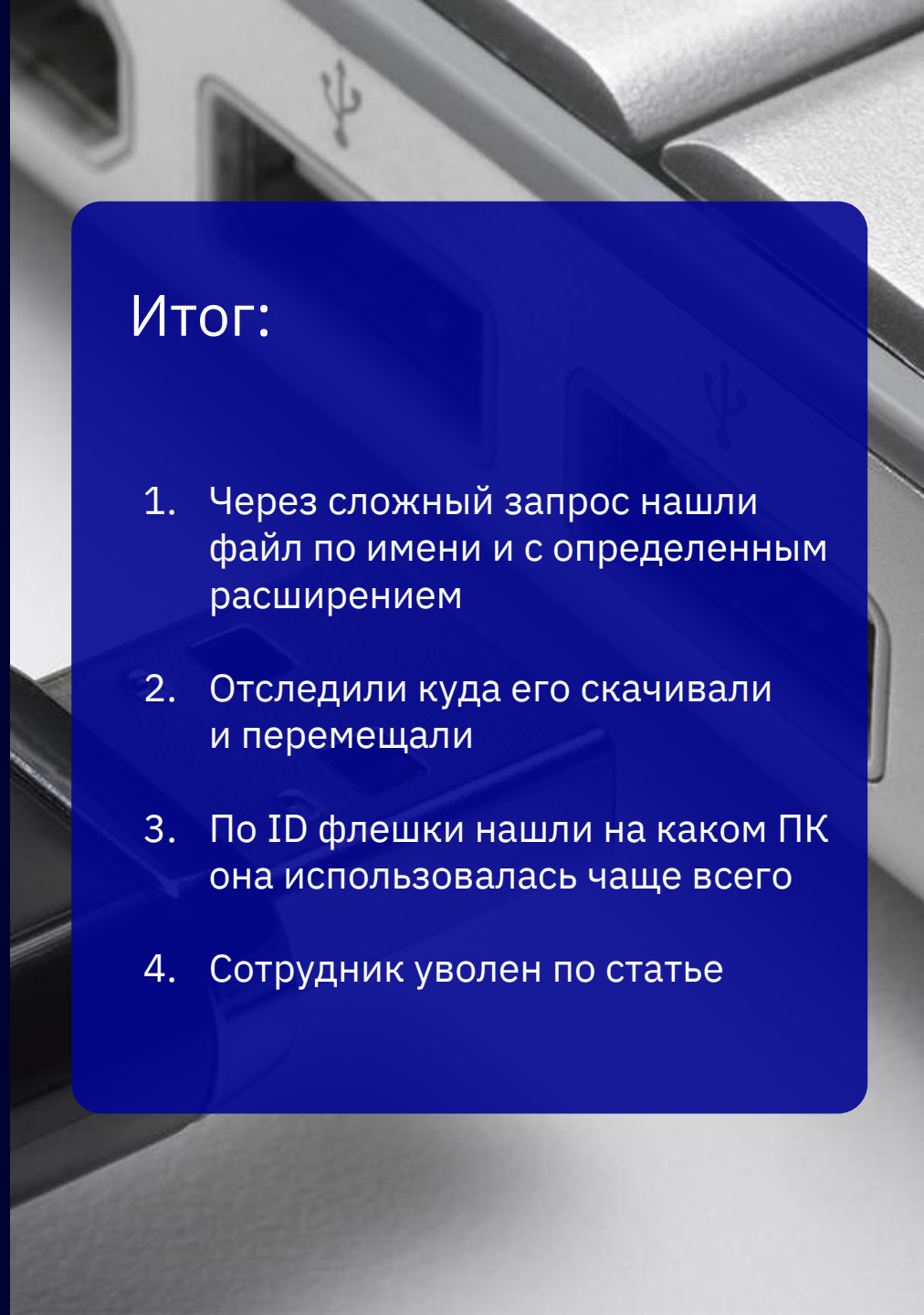
Итог:

1. Пометили файл специальной меткой
2. Отследили кто открывал и куда отправлял.
3. Выявили сотрудника, который передавал данные конкурентам

staffcop®

Кейс: Скачал файлы на флешку с ПК коллеги (Автодилер, 800 ПК)

1. Кто: менеджер отдела продаж
2. Узнал пароль от ПК коллеги
3. Знал, что стоит Staffcop!
4. Скачал файлы перед увольнением с ПК коллеги
5. Компания могла понести значительный финансовый ущерб



Итог:

1. Через сложный запрос нашли файл по имени и с определенным расширением
2. Отследили куда его скачивали и перемещали
3. По ID флешки нашли на каком ПК она использовалась чаще всего
4. Сотрудник уволен по статье

Если у вас уже есть DLP решения

Эшелонированная защита

DLP на шлюзе.
Staffcop на end point

На одной группе риска DLP.
На другой - Staffcop

Оптимизируйте бюджет защиты ИБ

Обеспечим защиту ваших филиалов

staffcop®

Преимущества Staffcop Enterprise

- 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

staffcop®

Попробуйте!

Отдел продаж
+7 (499) 653 71 52

sales@staffcop.ru

Спасибо за внимание!

Янушко Сергей

Старший менеджер отдела по работе
с партнерами ООО «АТОМ БЕЗОПАСНОСТЬ»

staffcop®

staffcop.ru

Telegram