Контроль над информационными потоками и действиями сотрудников как актуальная потребность бизнеса.

Даниил Бориславский
Аналитик ИБ, специалист
по внедрению
ООО Атом Безопасность

STAFFCOP

- Более 10 лет разработки приложений контроля сотрудников;
- Академгородок, Новосибирск, резиденты Технопарка и Сколково;
- Высокотехнологичная компания, ~50 сотрудников.
- Наша цель: «доступные решения задач информационной безопасности»
- ~100 серверных компонентов в месяц; ~ 94 000 АРМ за 2019-й год.

www.amtestlab.ru CERTIFIED AM TEST LAB REG # 00158 02/2016

PC MAGAZINE RUSSIAN EDITION BEST 2010 SOFT

академпарк
Технопарк Новосибирского Академгородка

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

Минкомсвязь России

infosecurity RUSSIA

BIS SUMMIT 2018

Где предприятия теряют деньги?

- Утечки информации: умышленные и неумышленные.
- Злоупотребления, мошенничество, фрод.
- Нецелевое и неэффективное использование рабочего времени.
- Отсутствие сотрудников на рабочем месте.
- Внутренние конфликты в коллективе.
- Кража и подмена комплектующих ПК.

Утечки информации

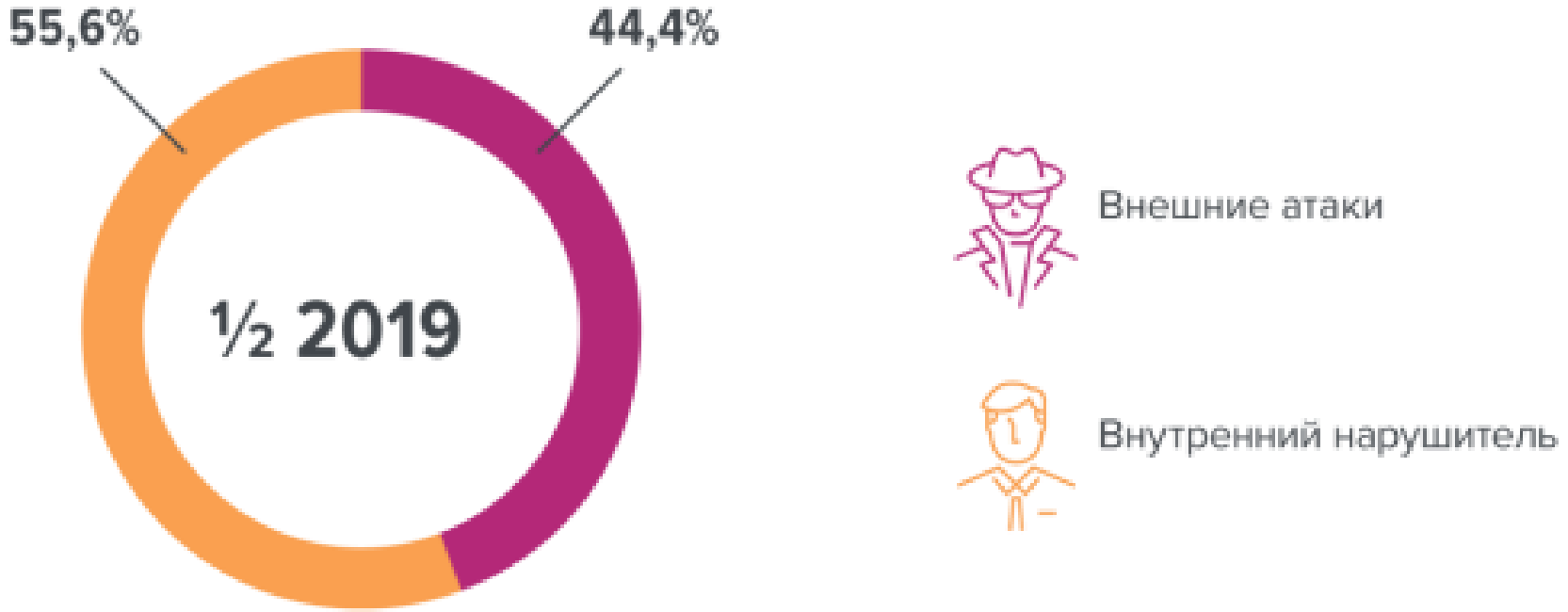


Рисунок 2. Распределение утечек по вектору воздействия[10], ½ 2019 г.

Утечки информации

Рисунок 6. Распределение утечек по каналам, ½ 2018 – ½ 2019 гг.

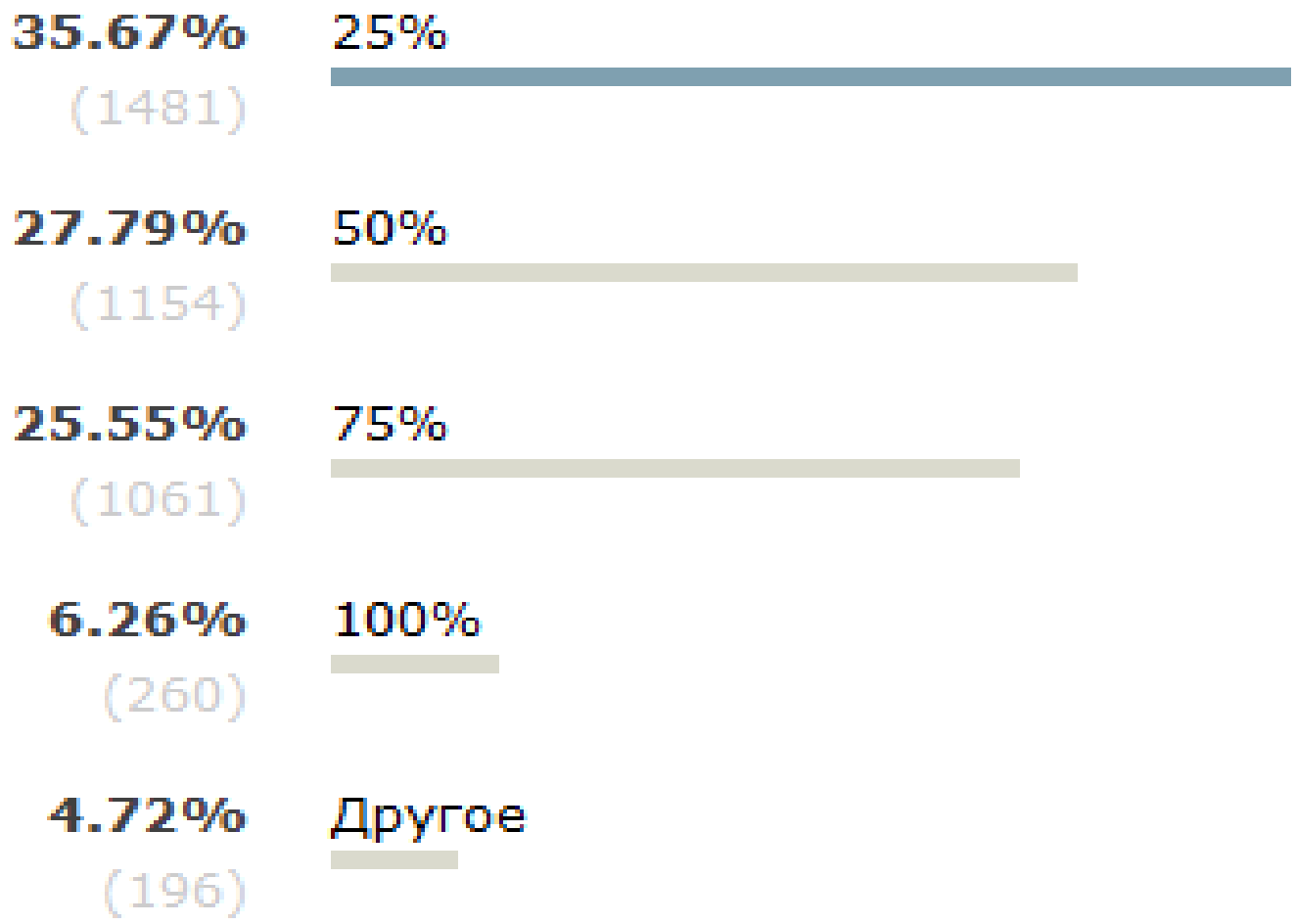
Злоупотребления, мошенничество, фрод

Учёт рабочего времени

9:00
В офисе
начало
рабочего дня

17:45
В офисе
заканчивается
рабочий день

Сколько времени вы реально работаете на работе?



Где предприятия теряют деньги?

50 сотрудников

Средний оклад 150 000 ₸

ФОТ 7 500 000 ₸ в месяц

5% «в холостую» - это 375 000 ₸ **в месяц!**

\+ недополученная прибыль от неэффективной работы

STAFFCOP

Комплексное решение по информационной безопасности,
учёту рабочего времени и контролю эффективности сотрудников

учет рабочего времени

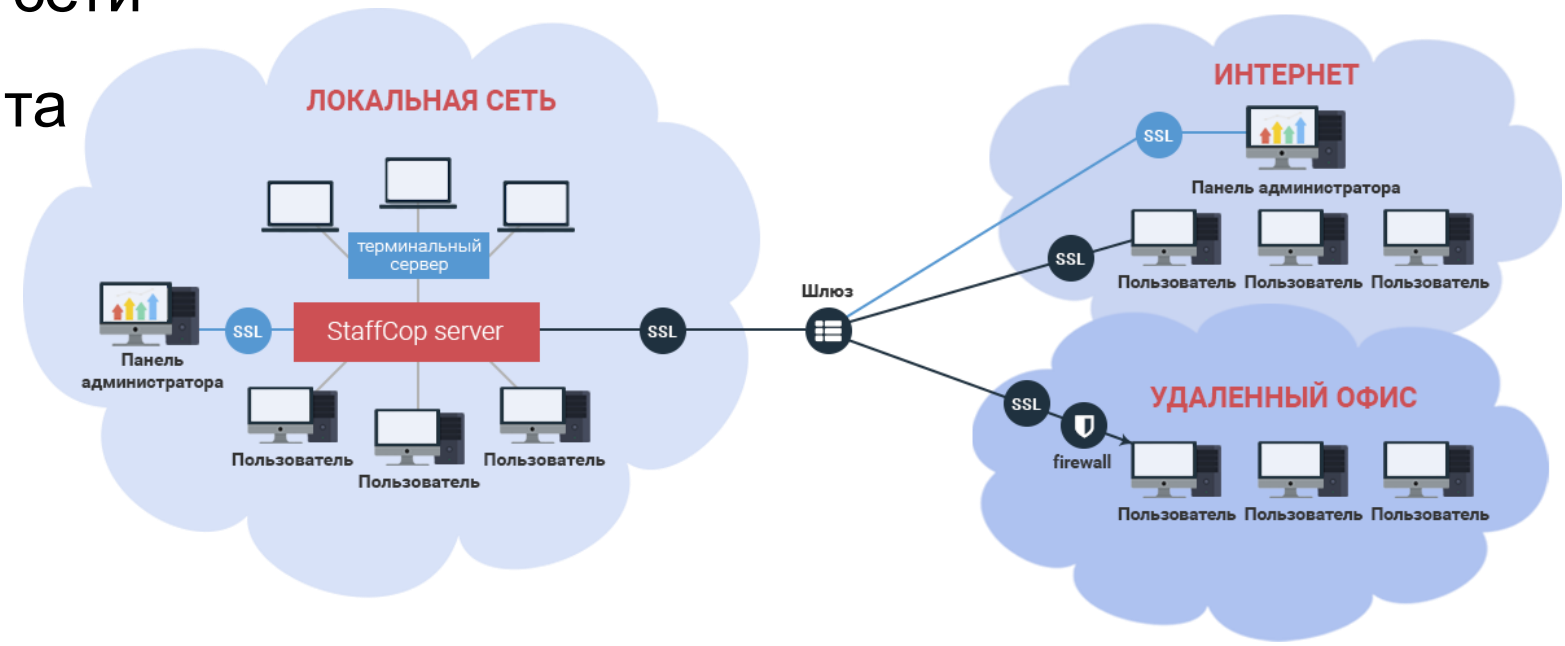
эффективность персонала

информационная безопасность

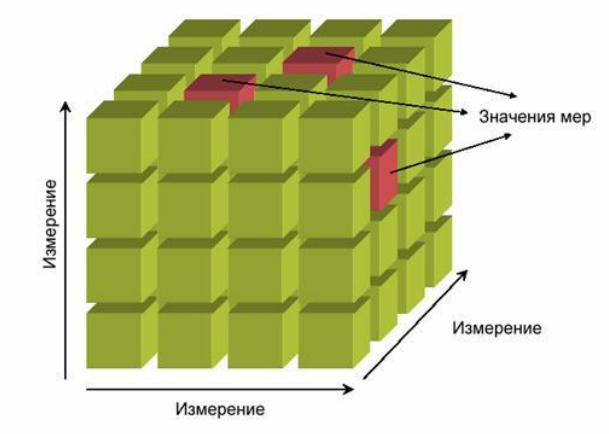
расследование инцидентов

Современные архитектурные решения

- Для установки сервера достаточно всего одной виртуальной машины на вашем ПК
- Система готова к сбору данных сразу после установки
- Работа в распределённой сети
- Удалённая установка агента



Современные архитектурные решения



OLAP технология. OnLine Analytical Processing — оперативный анализ данных

- Контроль ПК под управлением OS Windows, Linux, MacOS
- Единая консоль управления
- Одна база данных
- Нет дополнительных расходов за использование системы
- Гибкая настройка каналов перехвата
- OLAP технология

Современные архитектурные решения

Linux

— бесплатно

— менее требователен к «железу»

— заказчик может в любой момент забрать проект себе и доработать его собственными силами

Windows

— дорогие лицензии

— дорогое обслуживание

— высокие требования к «железу»

Тотальный контроль действий за ПК

Декодирование сервисов веб-почты и социальных сетей:

— mail.ru, yandex.ru, gmail.com…
— VK, FB, Одноклассники, LinkedIn…

Почтовые протоколы:
— SMTP / SMTPs
— IMAP
— POP3 / POP3s
— MS Exchange

Передача гипертекстовой информации и файлов:
— HTTP / HTTPs
— FTP / FTPs

Интернет-мессенджеры
— Skype
— ICQ, QIP, Jabber (XMPP)
— Mail.ru Agent
— Yahoo и другие

USB-порты
— контроль и блокировка

Теневое копирование файлов
— из электронной почты
— со съемных носителей
— переданных через интернет
— отправленных на печать

Расследование инцидентов ИБ

- **Архив данных**

все выбранные для контроля события попадают и остаются в системе; они доступны для анализа в любое время, в том числе и в ретроспективе.

- **Конструктор многомерных отчетов**

позволяют «налету» получить необходимый набор данных.

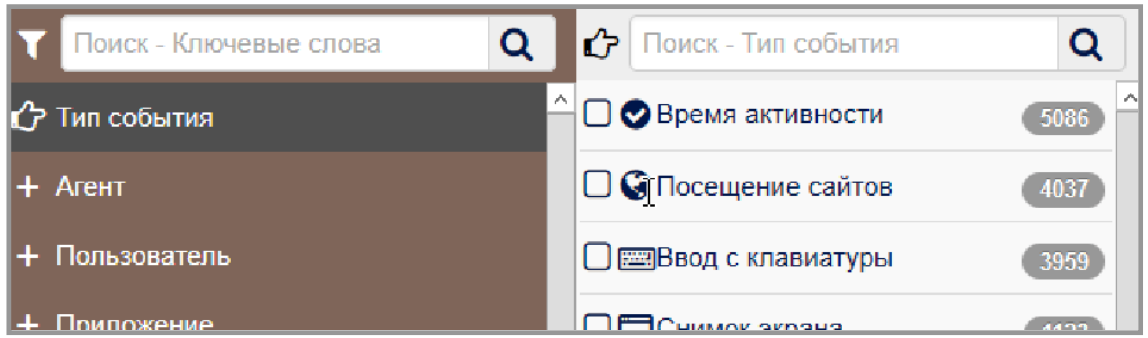
- **Поиск по словам и регулярным выражениям**

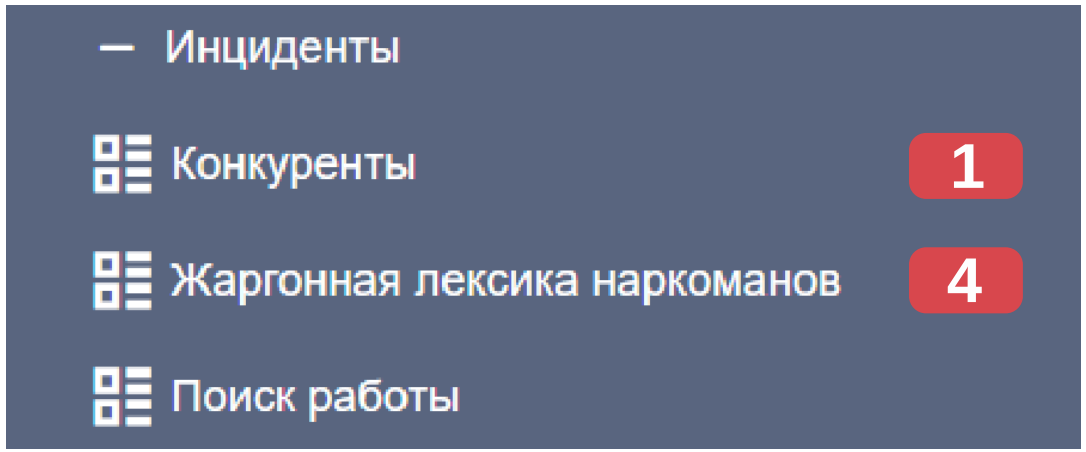
сокращает время расследования инцидента.

- **Множество графов и диаграмм**

линейные, круговые и тепловые диаграммы, графы взаимосвязей и т.д. позволяют визуализировать данные в наглядном информативном виде.

Обнаружение инцидентов и оповещения





- **Предустановленная категоризация событий**

Ускоряет процесс поиска событий

- **Контентный анализ файлов**

парсинг файлов на наличие в них конфиденциальной или потенциально опасной информации.

- **Система оповещений**

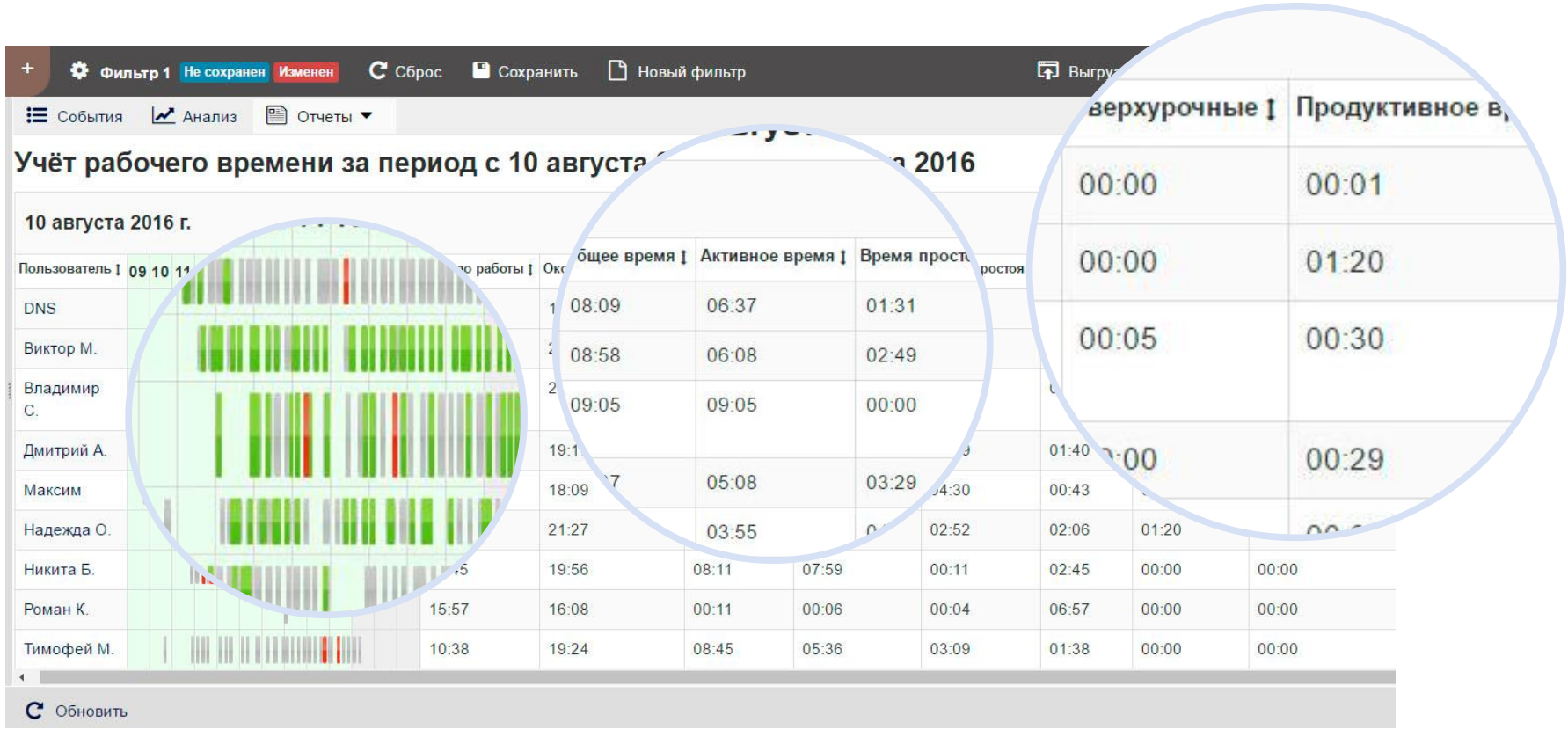
уведомления о нарушениях появляются как в панели администрирования, так и могут быть немедленно отправлены по электронной почте.

- **Гибкая система настройки фильтров**

позволяет не тратить время на лишнюю информацию; даёт возможность «на лету» менять критерии отбора.

Учёт рабочего времени и его оценка

- Продуктивная деятельность
- Непродуктивная деятельность
- Нейтральная деятельность
- Не было активности



Дисциплина Активность Эффективность

Управление и администрирование

- **Мониторинг**

— удаленный рабочий стол

— сетевой трафик

— процессы и приложения

— установка и удаление ПО

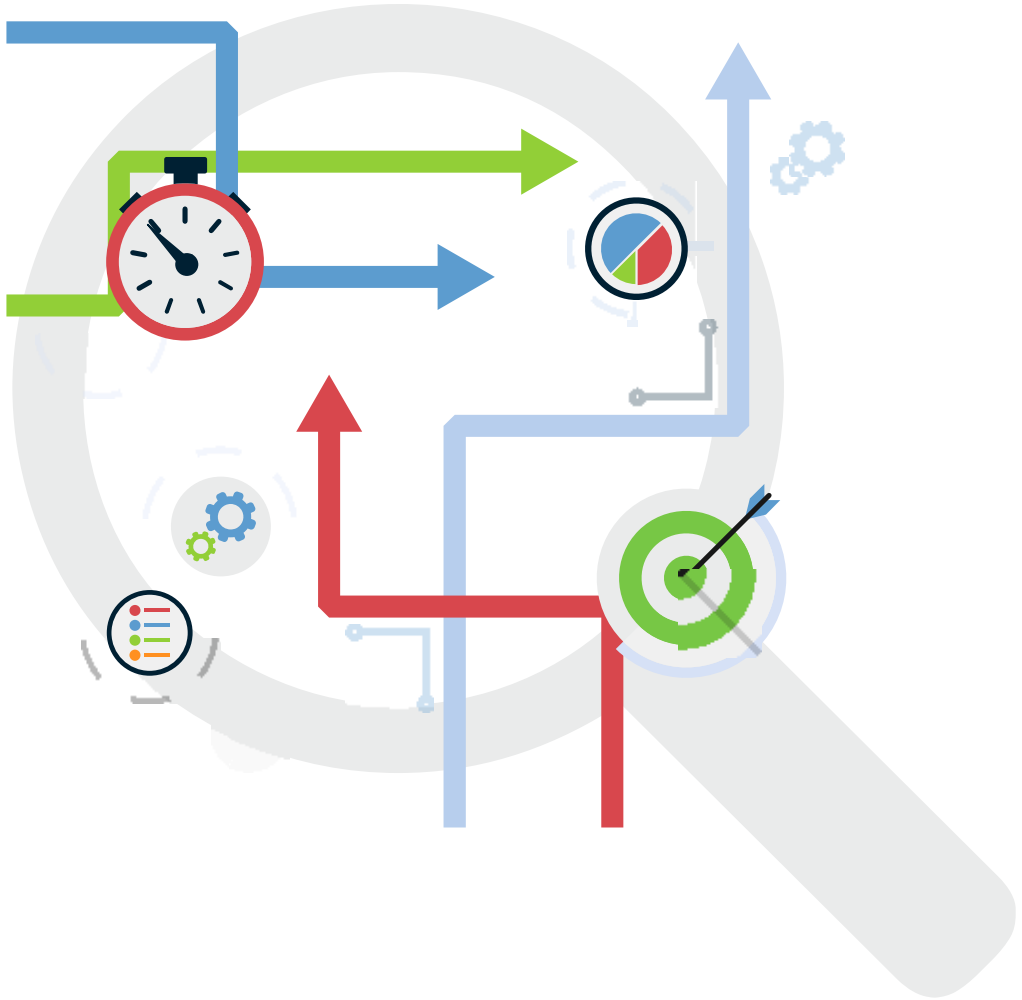
- **Блокировки**

— приложений и сайтов

— съемных USB-устройств

- **Инвентаризация ПО и «железа»**
- **Интеграция с SIEM**

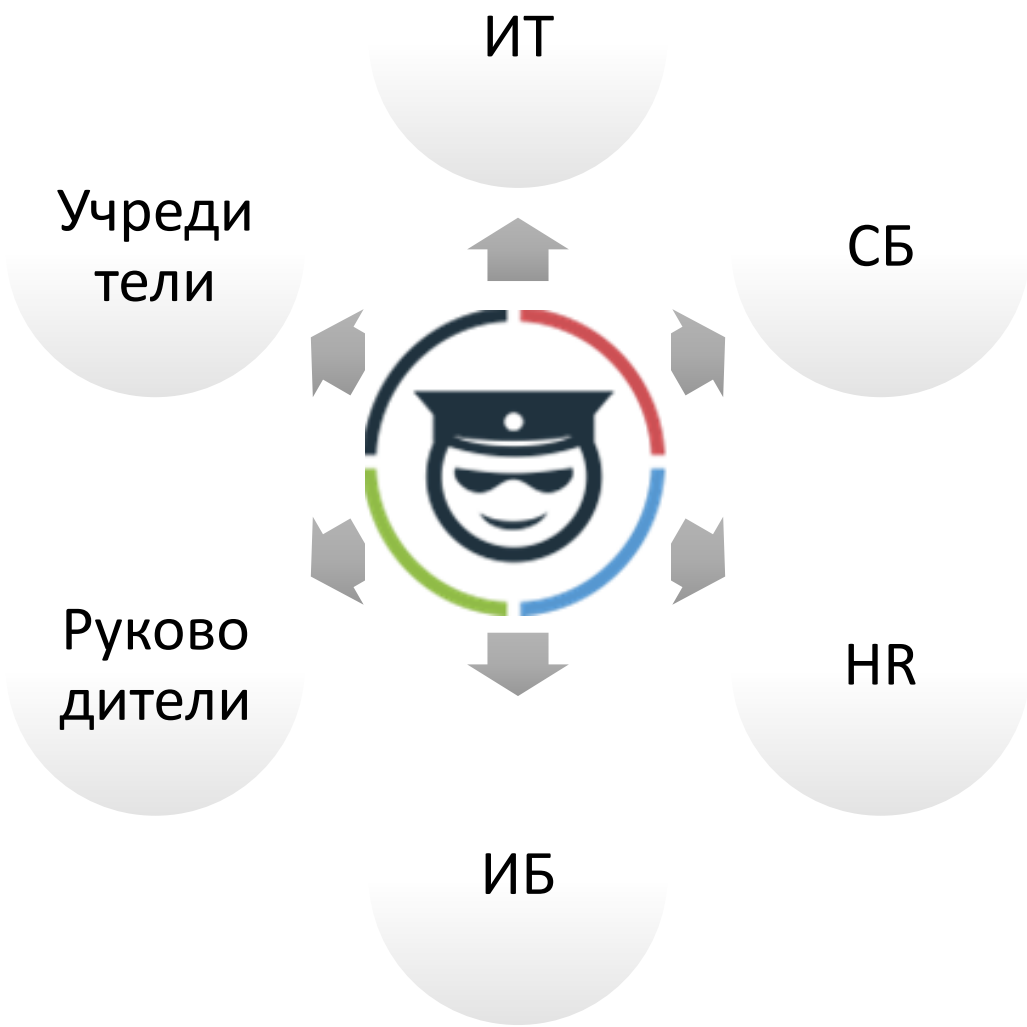
Оптимизация бизнес-процессов



Со StaffCop легко контролировать ваши бизнес-процессы, находить «узкие» места и выявлять блокирующие факторы, а также расследовать причины их появления.

Отслеживать реальный KPI сотрудников, например, для менеджеров продаж - это может быть количество отправленных коммерческих предложений и договоров, количество контактов с клиентами и поставщиками.

Потребители продукта



Обоснование для внедрения

Аспекты внедрения

Правовые

Обоснованием для внедрения являются

№149 ФЗ «Об информации, информационных технологиях и о защите информации».

№98 ФЗ «О коммерческой тайне».

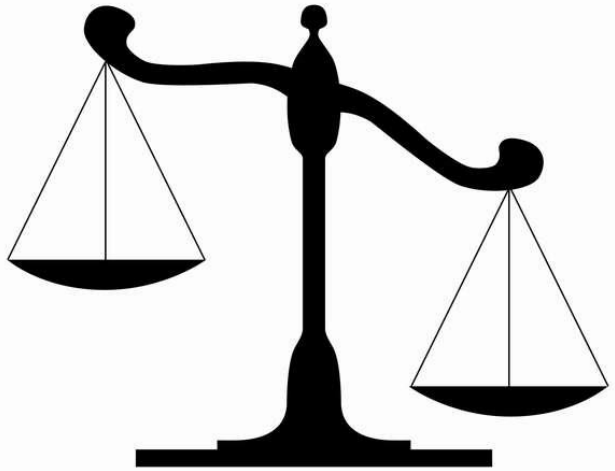
№152 ФЗ «О защите персональных данных».

Внутренняя организационно-правовая документация:

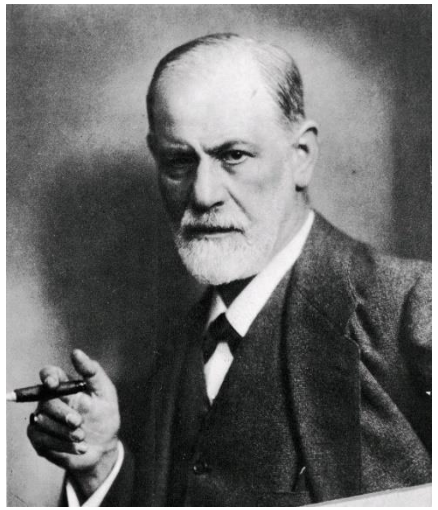
- стандарт по информационной безопасности;
- юридические риски по использованию нелегального ПО;
- регламент использования стандартного списка приложений;
- защита от вредоносных программ;

Аспекты внедрения

Правовые



Этические и психологические



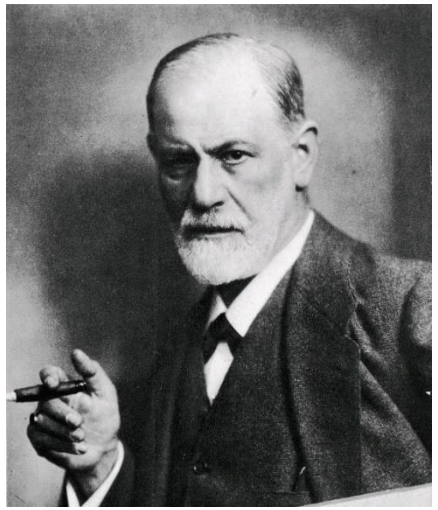
Обязательные действия перед началом мониторинга

- Определить и довести до работников правила использования средств хранения, обработки и передачи информации .
- Разработать и довести до работников регламент проведения мониторинга.
- Получить согласие работников на проведение мониторинга использования им средств хранения, обработки и передачи информации.
- Включить положения об обязательстве работника соблюдать правила использования средств коммуникации и согласие на мониторинг в трудовой договор (дополнительное соглашение к трудовому договору).

Аспекты внедрения

Правовые

Этические и психологические



Технические

Для успешного внедрения

- Определите цели
- Определите ответственных лиц
- Определите область контроля
- Подготовьте инфраструктуру
- Установите сервер Staffcop
- Внесите исключения в Антивирус
- Установите агентов
- Подведите итоги

Политика лицензирования и стоимость

Количество компьютеров	Бессрочная лицензия	Лицензия на 12 месяцев	Лицензия на 3 месяца
5–25	26 080 ₸ / 1 ПК	18 440 ₸ / 1 ПК	6 150 ₸ / 1 ПК
26–50	24 220 ₸ / 1 ПК	17 170 ₸ / 1 ПК	5 710 ₸ / 1 ПК
51–100	22 980 ₸ / 1 ПК	16 295 ₸ / 1 ПК	5 430 ₸ / 1 ПК
101–150	21 425 ₸ / 1 ПК	15 150 ₸ / 1 ПК	5 050 ₸ / 1 ПК
151–250	20 785 ₸ / 1 ПК	14 700 ₸ / 1 ПК	4 900 ₸ / 1 ПК
251–500	19 750 ₸ / 1 ПК	13 960 ₸ / 1 ПК	4 650 ₸ / 1 ПК
501–1000	19 150 ₸ / 1 ПК	13 544 ₸ / 1 ПК	4 515 ₸ / 1 ПК
1000+	18 195 ₸ / 1 ПК	12 870 ₸ / 1 ПК	4 325 ₸ / 1 ПК

Тестируйте бесплатно до 3-х месяцев на парке машин любого размера.

Полнофункциональная версия. Техническое сопровождение проекта на всем протяжении.

Быстро

Развертывание пилотного проекта обычно занимает не более одного дня

Легко

Требуется минимум усилий и ресурсов для запуска StaffCop Enterprise

Комплексно

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

Спасибо за внимание!

Даниил Бориславский
Аналитик ИБ, специалист по внедрению
ООО Атом Безопасность

+74996382809 доб. 235
d.borislavskiy@staffcop.ru
d.borislavskiy