staffcop®

Расследование инцидентов
внутренней безопасности

# Расследование инцидентов ИБ и контроль работы сотрудников

Курьянов Александр

Старший специалист отдела внедрения
ООО «АТОМ БЕЗОПАСНОСТЬ»

staffcop

# О компании

Единая консоль и многомерная архитектура данных позволяют расследовать любой инцидент за несколько кликов

**11+ лет**

Разработки приложений контроля сотрудников

**Лучшее ПО для мониторинга сотрудников**

По версии Forbes Advisor, 2023 г.

Импортонезависимый продукт. Российский разработчик

**100 +**

Сотрудников

**200**

Конференций, в которых мы приняли участие за 3 года

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

4 уровень доверия

АРПП Отечественный софт

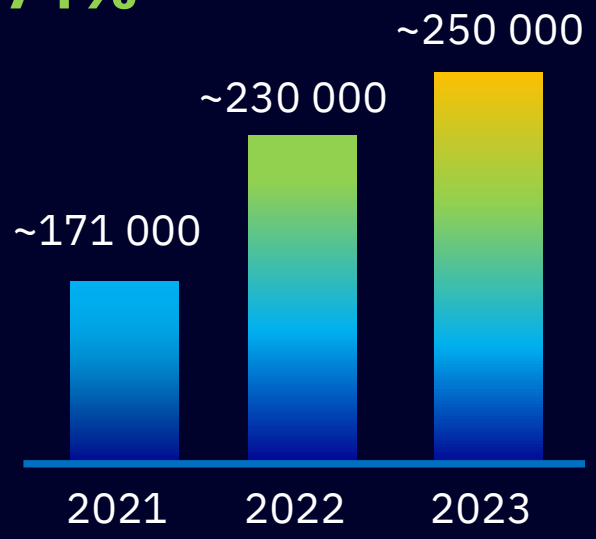
Минцифры России

Sk Участник

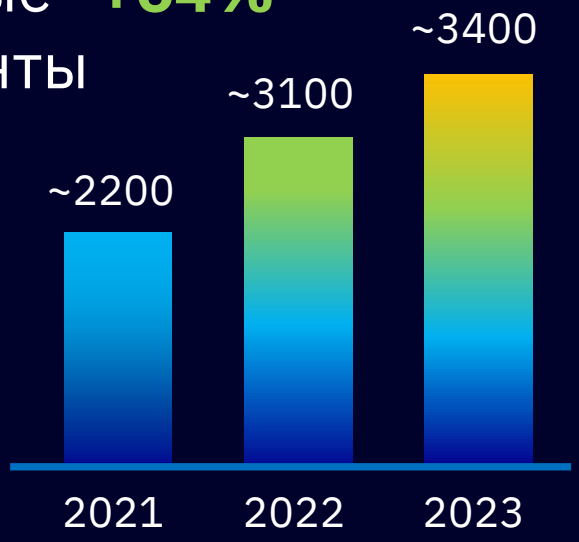
академпарк

# О компании

ARM **+74%**




Серверные компоненты **+64%**




Клиенты:

**20+ клиентов из Топ 100 Forbes**

ЛУКОЙЛ · НЦВ Миль и Камов, Холдинг вертолеты России · Ростех · ДОМ.РФ БАНК

staffcop

# Риски внутренней безопасности. Угрозы от инсайдеров

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

# Актуальное законодательство

staffcop

## Уже есть

- **Указ 250:** персональная ответственность руководителя за состояние ИБ в организации
- **ФЗ 152:** необходимо сообщить об инциденте утечки ПДн в течение суток
- **ФЗ 152:** необходимо предоставить результаты расследования инцидента утечки ПДн в течение трёх суток
- **ФЗ 187:** ряд обязательных мер для предприятий КИИ
- Импортозамещение

## Готовятся

- Оборотные штрафы за утечку ПДн
- Уголовная ответственность за «продажу» ПДн
- Правительство само будет определять объекты КИИ

# Решаемые задачи

## 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

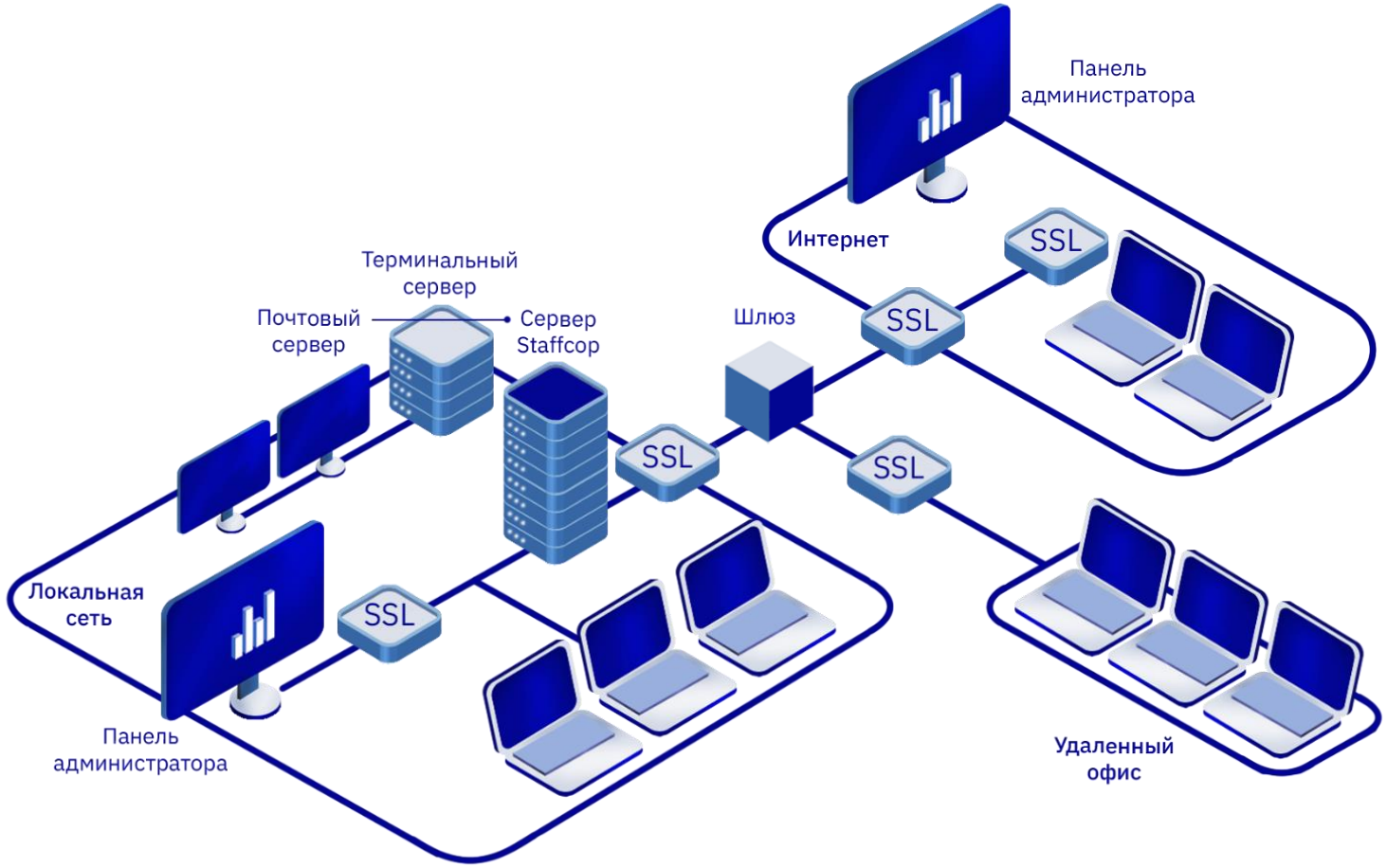
- Удаленное администрирование
- Инвентаризация компьютеров
- Индексирование файлов на ПК

## 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
- Импортонезависимое ПО
- Масштабированная архитектура
- OLAP технология хранения данных



# Использование отечественного и независимого ПО

staffcop

## Технологии сервера:

open source initiative

ASTRA LINUX®

ClickHouse

PostgreSQL

## OS рабочих ПК и АРМ:

base alt

ROSA

ОСНОВА

ASTRA LINUX®

РЕДОС

Компоненты, не требующие лицензирования и покупки

Собственникам бизнеса | IT специалистам | Сотрудникам HR | ИБ специалистам

staffcop

# Аналитические возможности

**01** Архив данных

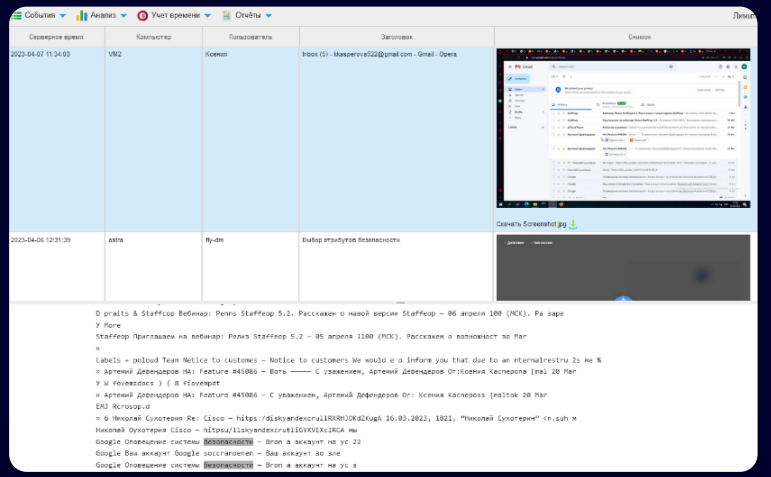
**02** Поиск по словам и регулярным выражениям

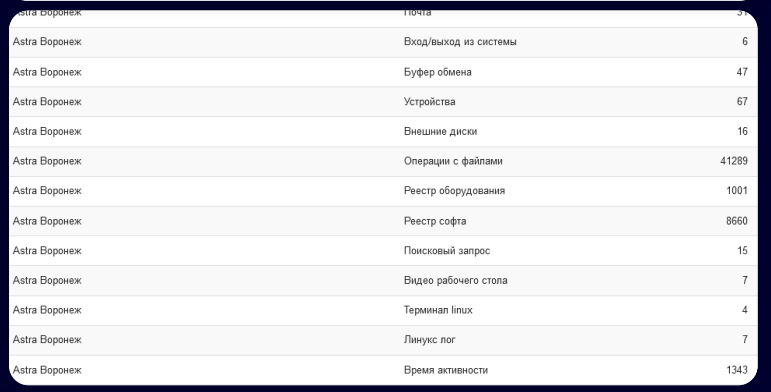
**03** Синхронизация данных с AD

**04** Конструктор многомерных отчетов

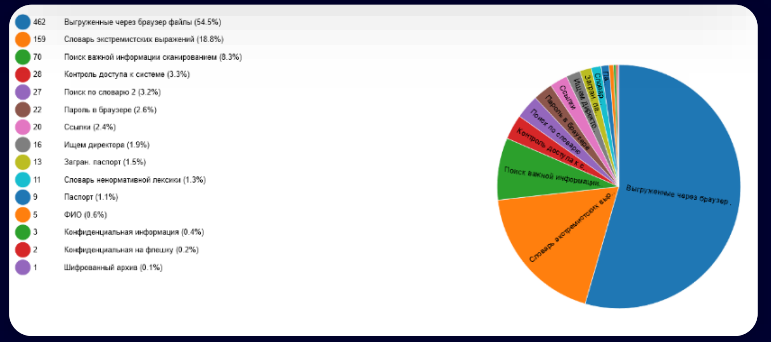
**05** Множество графов и диаграмм

**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 |



Собственникам бизнеса

ИБ специалистам

staffcop

# Расследование инцидентов ИБ

**01** Система оповещений

**02** Гибкая система настройки фильтров

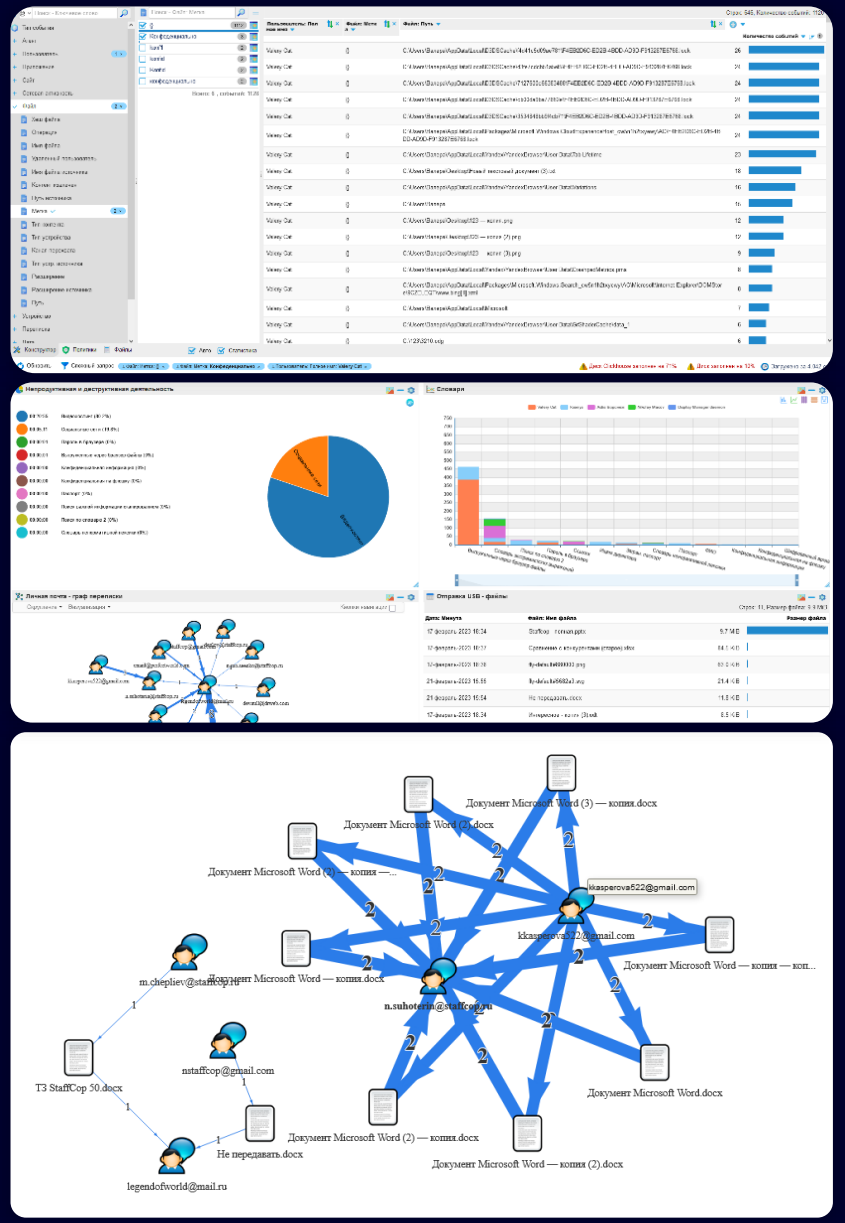
**03** Графы взаимосвязей

**04** Метки для файлов

**05** Изменение конфигурации контроля при наступлении определённого события

**06** Защита от массового копирования

**07** Нейронная сеть распознавания изображений

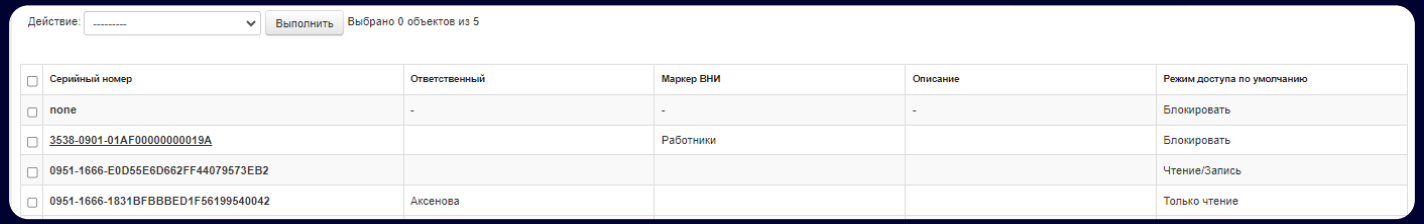


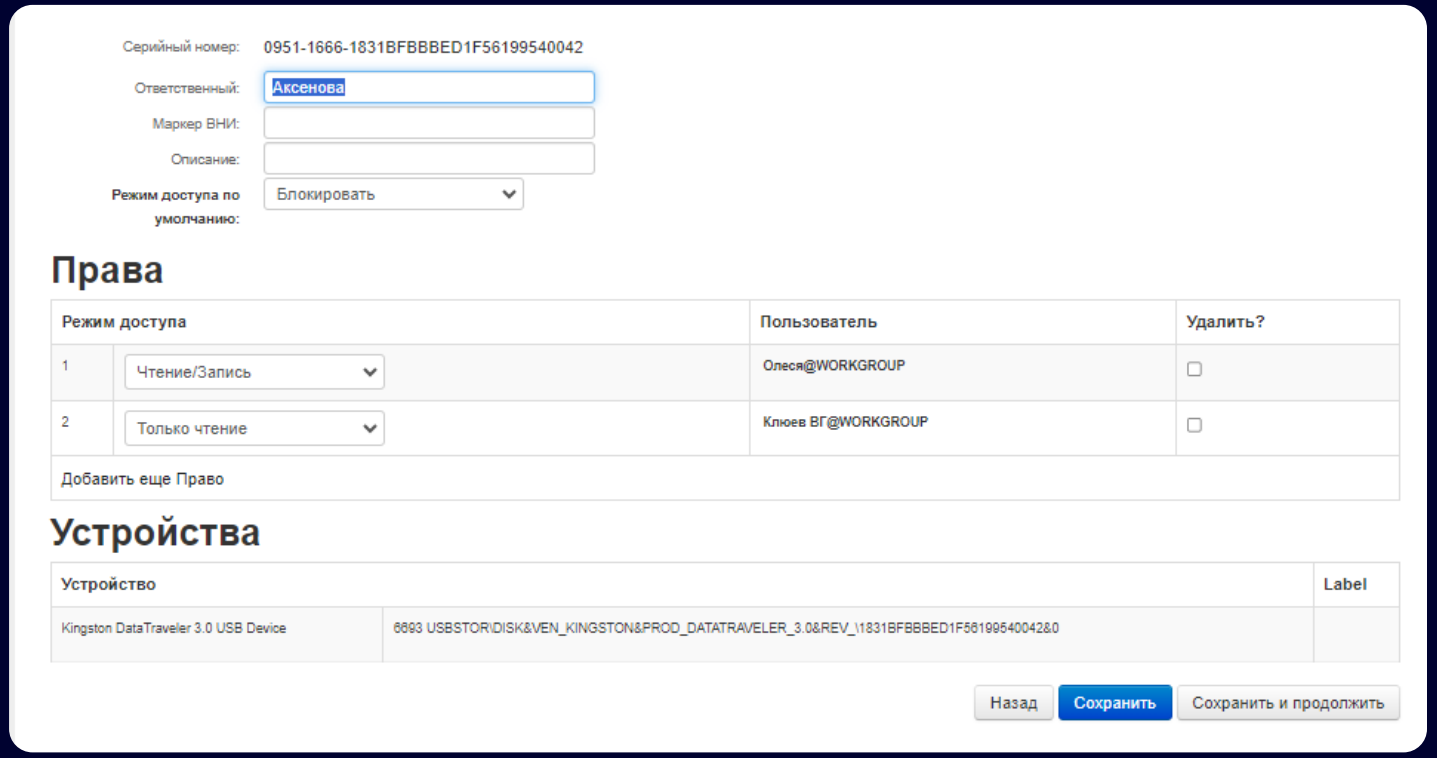
# Менеджер ВНИ

**01** Гибкое назначение прав

**02** Автоматическое назначение доступа неавторизованным накопителям

**03** Назначение ответственных за устройство



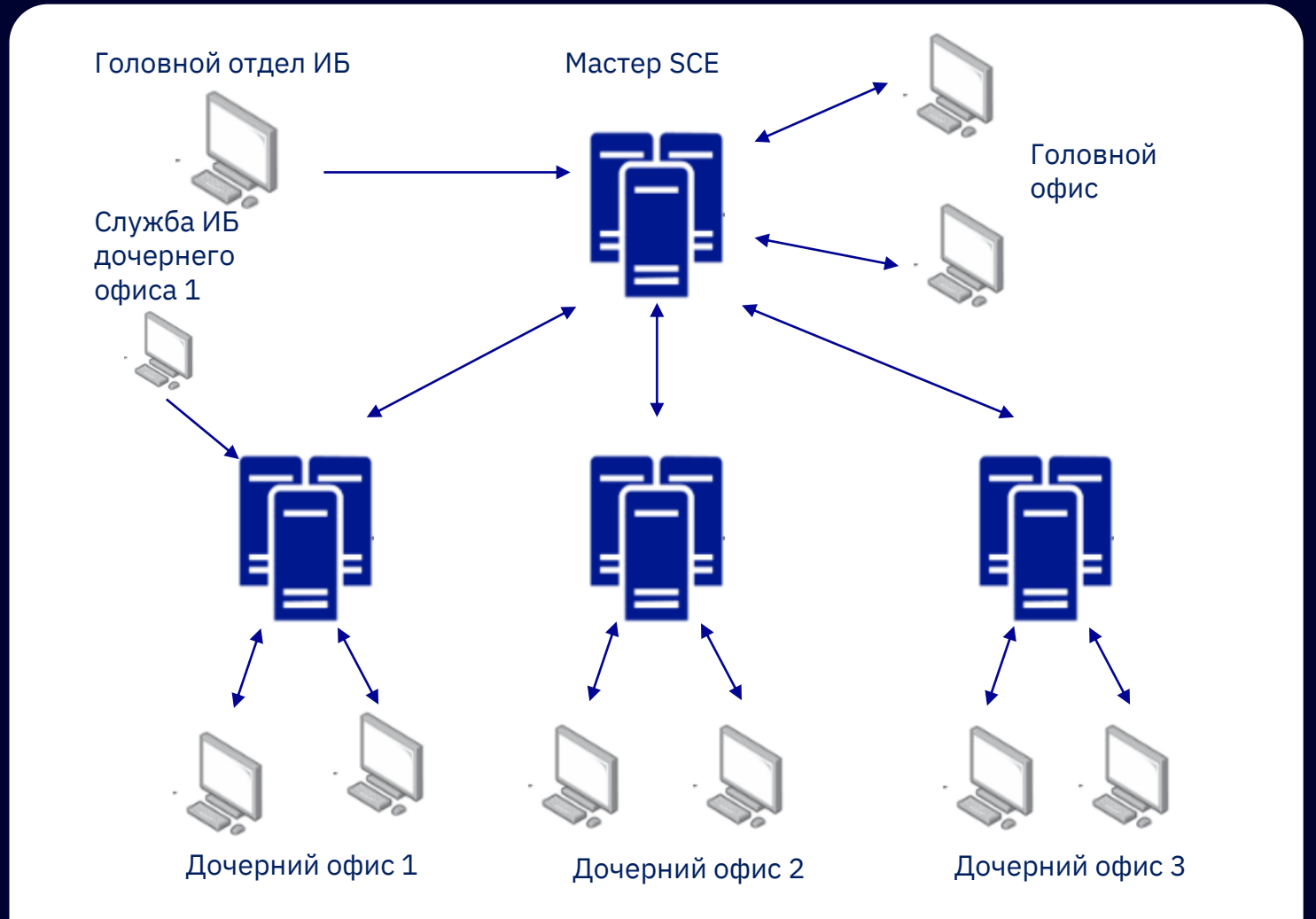
# Горизонтальное Масштабирование

staffcop

**01** Распределение нагрузки

**02** Сегментирование на зоны

**03** Централизованное управление



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

# Если у вас уже есть DLP решения

Эшелонированная защита

На одной группе риска DLP.
На другой - Staffcop

DLP на шлюзе.
Staffcop на end point

Оптимизируйте бюджет защиты ИБ

staffcop

# 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!

# В Staffcop 5.3:

- Менеджер внешних носителей информации
- Карточка сотрудника
- Новый сервис мониторинга агента
- Новый каналы перехвата
- Новые и действующие клиенты выбирают нас

# Спасибо за внимание!

Курьянов Александр

Старший специалист отдела внедрения
ООО «АТОМ БЕЗОПАСНОСТЬ»

staffcop®

staffcop.ru

Telegram