# IRM: инсайдеры все ближе... Инцидентов все больше...

Юрий Драченин

Заместитель генерального директора
ООО «Атом Безопасность»
duu@staffcop.ru

Контур staffcop

# О компаниии

**>12 лет**

Экспертизы в информационной безопасности

**>3000**

Клиентов в 40+ странах мира

**>250 тыс**

ПК под защитой Staffcop

**>20**

Клиентов из Top списка Forbes

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

Forbes ADVISOR

Лучшее ПО по версии
Forbes Advisor 2023 и 2024

СКБ Контур

Входим в ГК СКБ Контур

Импортонезависимый продукт.
Российский разработчик

ФСТЭК России
Федеральная служба по
техническому и экспортному контролю

4 уровень доверия

АРПП
Отечественный софт

Минцифры России

Sk Участник

РУС СОФТ

# Клиенты

## 20+ клиентов из Топ 100 РБК

# Актуально

>66%

# Немного цифр

**+80%** утечек к 2023

По кол-ву инцидентов:

- 1. Розничная торговля
- 2.Сфера услуг
- 3. Гос сектор

По кол-ву информации:

- 1. Финсектор – x3
- 2. Ритейл]
- 3. Услуги

# Актуально

Станислав Кузнецов (Сбер):

**1**

трлн рублей

**250**

млрд рублей

# Оборотно

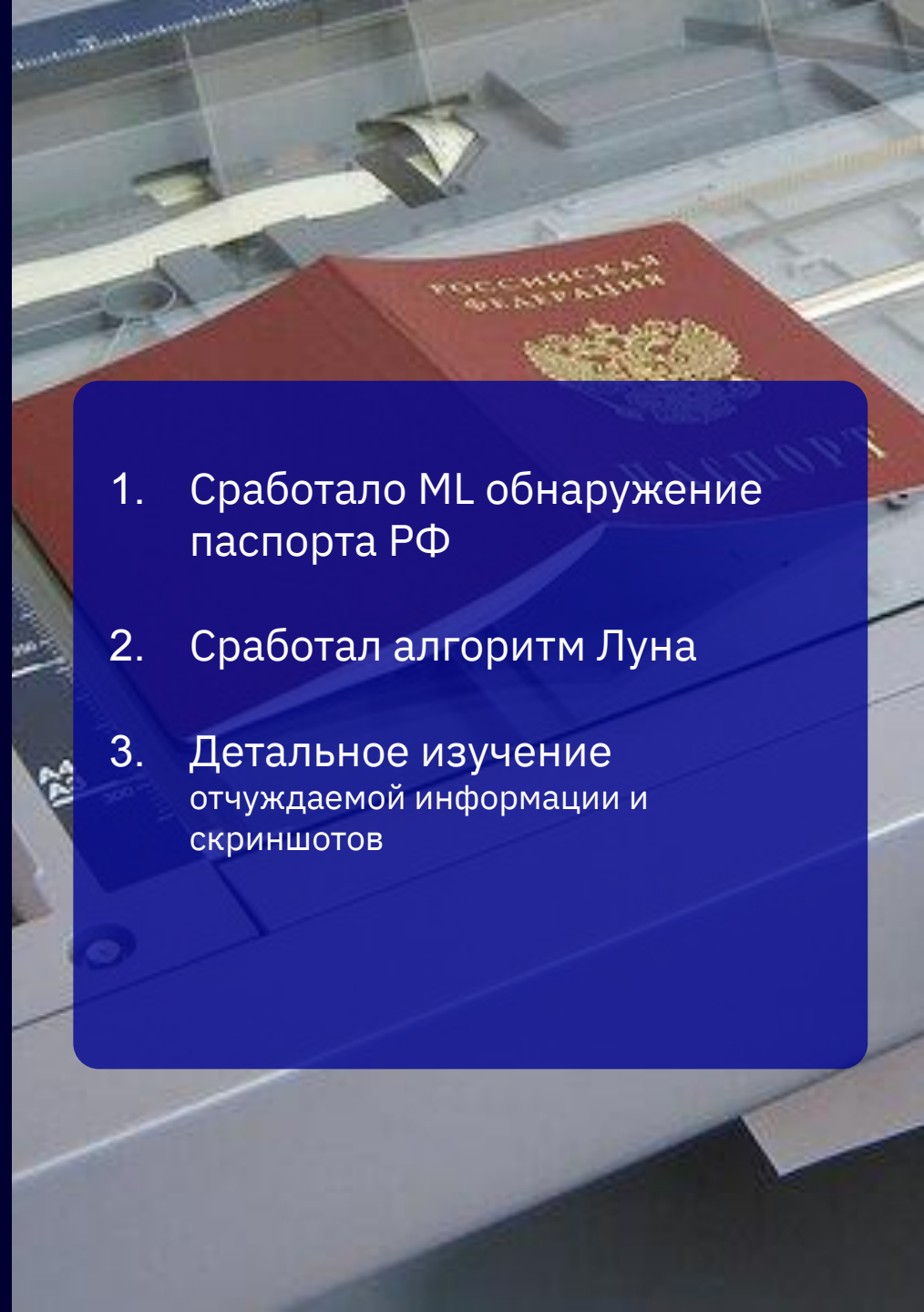
«Количество утечек ПДН превышает
все допустимые пределы»

М.И.Шадаев

# Инсайдеры - доступней не придумаешь...

# Кейс: утечка скана паспорта и номера карты

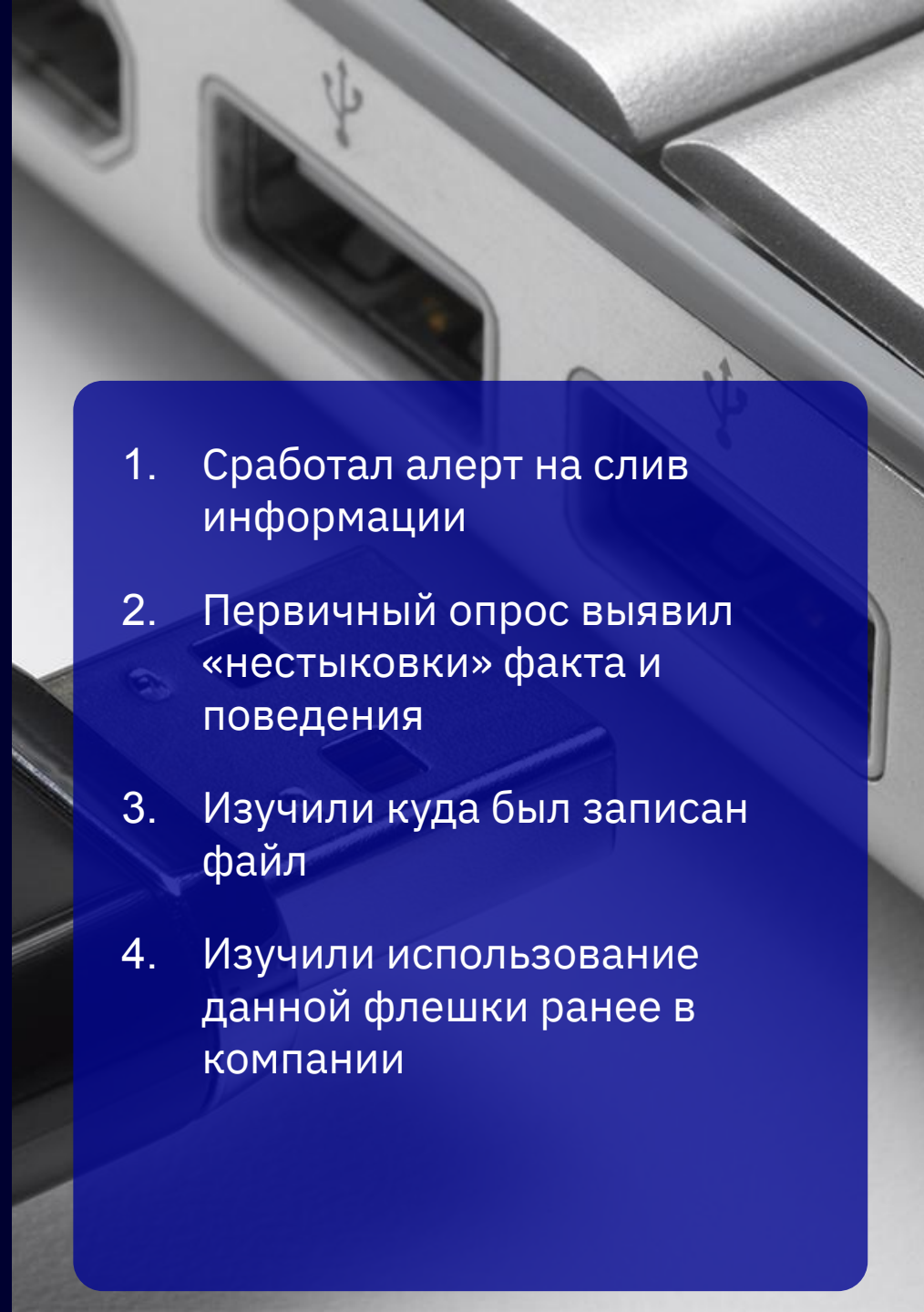
1. Кто: сотрудница банка
2. Отправляла с личной почты и через мессенджеры сканы паспорта и номера карт клиентов
3. Передавала данные третьему лицу




1. Сработало ML обнаружение паспорта РФ
2. Сработал алгоритм Луна
3. Детальное изучение
   отчуждаемой информации и скриншотов

# Кейс: скачал файлы на флешку с ПК коллеги

1. Кто: просто сотрудник
2. Планировал увольнение
3. Знал, что в организации есть Staffcop
4. Узнал пароль от учётки коллеги
5. Скачал файлы с ПК коллеги



1. Сработал алерт на слив информации
2. Первичный опрос выявил «нестыковки» факта и поведения
3. Изучили куда был записан файл
4. Изучили использование данной флешки ранее в компании

I

Insider

R

Risk

M

Management

# Расследование инцидентов. Сбор доказательной базы

- Утечка информации. Потеря данных
- Предупреждение опасных действий и мошеннических схем сотрудников
- Риски, связанные с удаленной работой
- Контроль периферийного оборудования и ПО
- Дисциплина сотрудников
- Возможность сбора доказательной базы

# Импортонезависимость - почему именно сейчас это реально важно?

# Использование отечественного и независимого ПО

**Технологии сервера:** компоненты, не требующие лицензирования и покупки

ASTRA LINUX

open source initiative

ClickHouse

Jatoba

PostgreSQL

---

**OS рабочих ПК и АРМ**

ASTRA LINUX

РЕДОС

SIEM

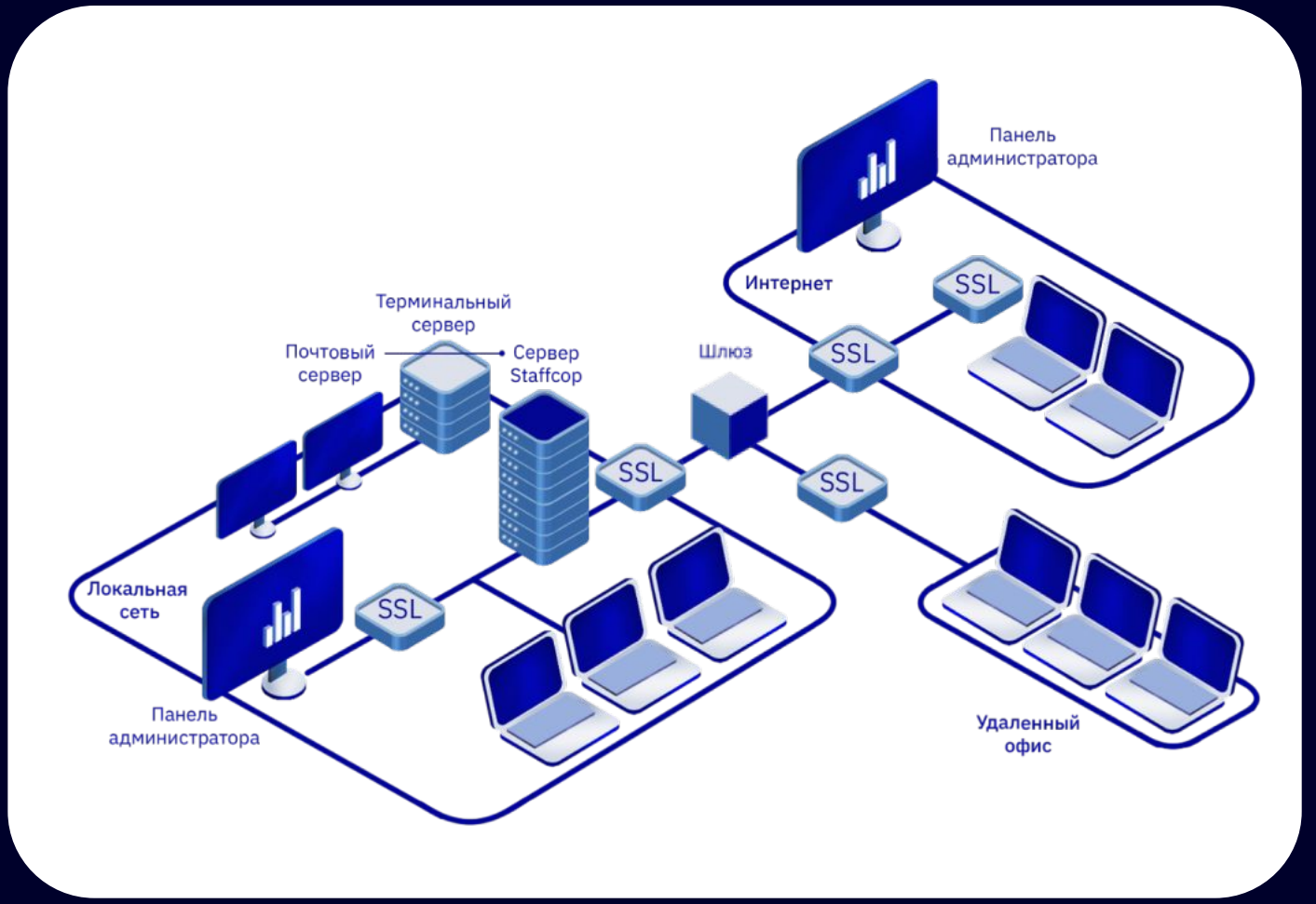
ROSA

base alt

Ankey ASAP

# 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
- Масштабируемая архитектура
- OLAP технология хранения данных



# Сервисы информационной безопасности Контура

## staffcop®

Контроль и расследование инцидентов внутренней инфраструктуры

Автоматизированная система расследования внутренних инцидентов

## Контур ID

Безопасность корпоративных учетных записей сотрудников

Двухфакторная аутентификация

## Контур Доступ

Безопасное администрирование удаленных пользователей

Безопасный удаленный доступ

# Будущие сервисы информационной безопасности Контура

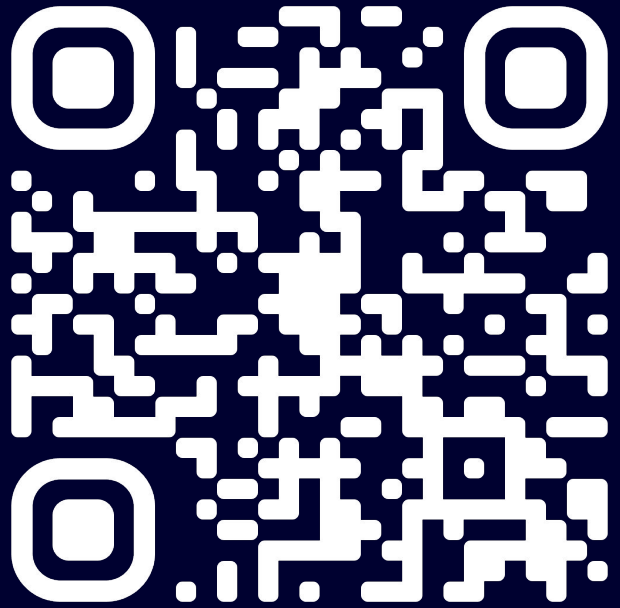
Безопасное массовое администрирование парка компьютеров

Защита критичных точек инфраструктуры

Сервис для системных администраторов

Сервис привилегированных пользователей

# Узнать больше и оставить заявку на тестирование продуктов ИБ



# Тестируйте уже сейчас!

## Быстро

Развертывание пилотного проекта обычно занимает не более одного дня

## Комплексно

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

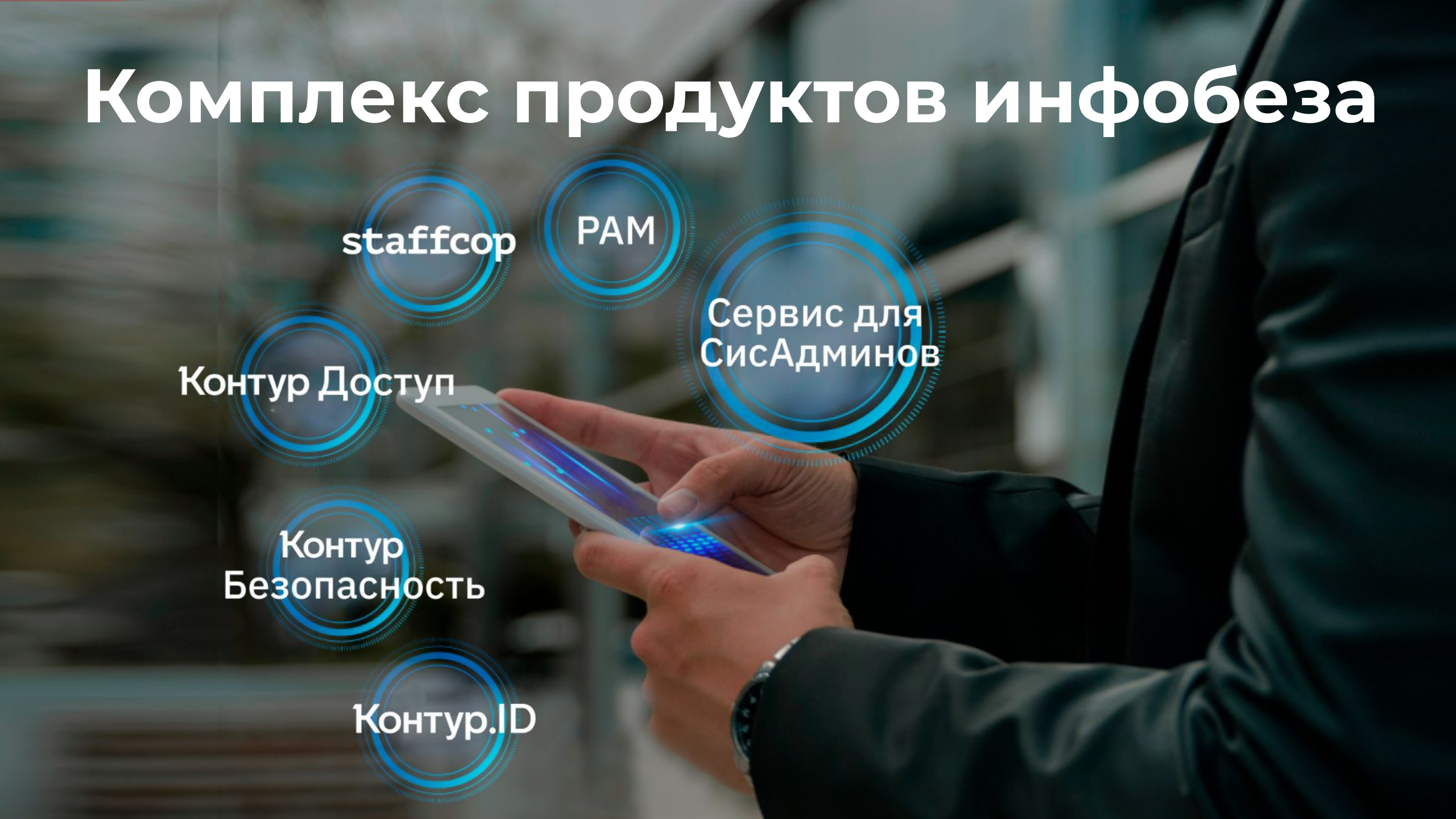
## Легко

Требуется минимум усилий и ресурсов для запуска

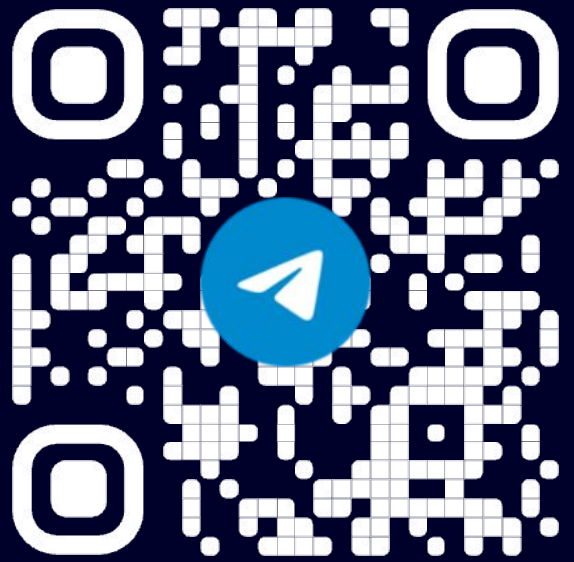
## Бесплатный аудит

Позволит вскрыть точки роста в Вашей системе ИБ

# Комплекс продуктов инфобеза



# Спасибо за внимание Вопросы?



telegram

Юрий Драченин

Заместитель генерального директора
ООО «Атом Безопасность»
duu@staffcop.ru

Контур staffcop