

Ответ Контура на рост спроса в сфере информационной безопасности

Дмитрий Мельников

Менеджер проектов по внедрению



Контур

kontur.ru

Боли рынка кибербезопасности

x3

Втрое выросла доля утечек информации категории «государственная тайна» (относительно 2022 года)

87%

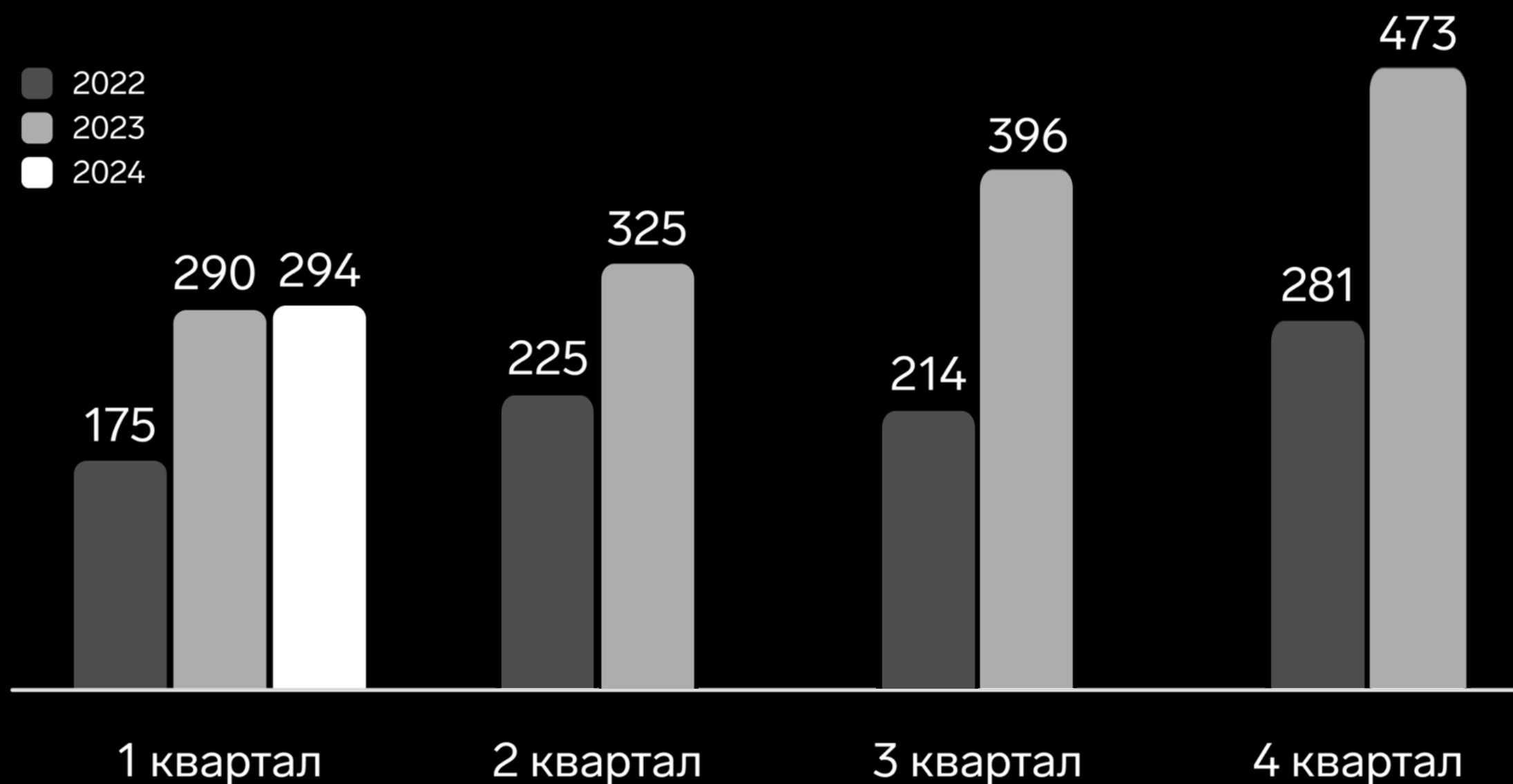
На одну утечку в среднем пришлось на 87% больше записей, чем в 2022 г.

>80%

Утечек информации произошли в результате кибератак

События информационной безопасности в РФ

Распределение событий ИБ по кварталам, тыс.



1,4 млн событий ИБ за 2023 год, что на 65% больше, чем в 2022 г.

По 1 кв. 2024 года — сохраняется тенденция по количеству событий 2023г.

по данным Ростелеком Солар

Распределение инцидентов 1 кв. 2024 г. по уровню критичности

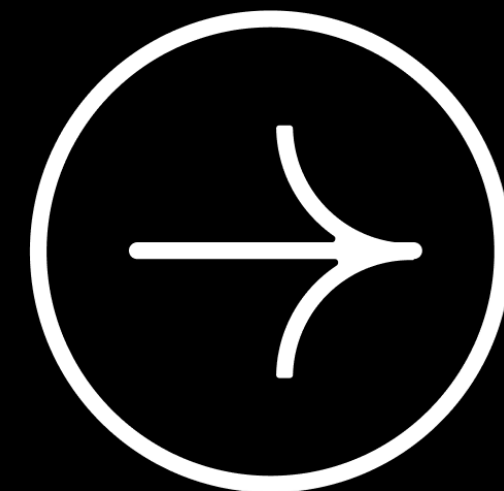
на 7%

увеличилась доля высокой степени критических инцидентов, что существенно превышает показатели последних лет (даже периода массовых атак на российские компании в начале 2022 года).

49%

Инцидентов высокой степени критичности — несанкционированный доступ к информационным системам и сервисам

**Рост угроз на рынке
кибербезопасности
формирует новые
потребности в защите
инфраструктуры
компании**



Основные направления

1

Контроль
и расследование
инцидентов внутренней
инфраструктуры

2

Безопасность
корпоративных
учетных записей
сотрудников

3

Безопасное
администрирование
удаленных
пользователей

Контур в ИБ

1 место

Среди SaaS-поставщиков России по объему выручки по итогам исследования CNews Analytics: Крупнейшие поставщики услуг SaaS 2022 года.

>5 000

Клиентов курируют безопасность компаний благодаря сервисам Контура

>250 000

Сотрудников компаний-клиентов пользуются сервисами ИБ

Staffcop

Система расследования инцидентов
внутренней безопасности



staffcop®

staffcop.ru

Расследование ИНЦИДЕНТОВ

- Локализация и ликвидация последствий инцидентов ИБ
- Установление виновных лиц и их мотивации, обеспечение возможности привлечения их к ответственности
- Анализ инцидентов и принятие мер по предотвращению подобных в будущем

Решаемые задачи

→ Эффективность работы персонала

- Оценка продуктивности сотрудников
- Мониторинг бизнес процессов

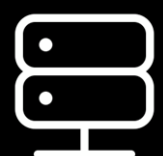
→ Администрирование рабочих мест

- Удаленное администрирование
- Инвентаризация компьютеров
- Индексирование файлов ПК

→ Информационная безопасность

- Раннее обнаружение угроз ИБ
- Расследование инцидентов
- Анализ поведение пользователей

Как работает staffcop?



Сбор данных

Агент собирает все события о действиях пользователя и движениях информации



Анализ

Визуальный и статистический анализ данных для выявления отклонений



Оповещение

Автоматическое оповещение о нарушении политики безопасности



Расследование

Поиск информации в любых событиях на основе морфологии фраз и регулярных выражений

staffcop[®]

Безопасный вход на корпоративные ресурсы

> 1,12 млрд

Скомпрометированных данных за 2023 г.
(на 60% больше, чем в 2022 г.)

15%

Всех атак приходится на попытку
скомпрометировать корпоративную
учетную запись

Контур.ID — двухфакторная аутентификация

Защита учетных записей сотрудников:
подключений через VPN, RDG,
ActiveSync, ADFS (протоколы OpenID
Connect, SAML), защита входа
в Windows, OWA



KONTUR.RU
ivanov@kontur.ru

947 583 

Контур ID

kontur.ru/id

Двухфакторная аутентификация



Защита корпоративных учетных записей

Защищает рабочие аккаунты
от взлома



Интеграция с веб-сервисами

Поддерживаем популярные
протоколы аутентификации openID
Connect, SAML



Защиты почты и ПК

Интеграция с outlook
и WinLogon



Отслеживание активности

Отслеживаем где и когда пользователь
использовал свою учётную запись

Контур ID

Сценарии для защиты

**RDP
(RDGW)**

ADFS

SSH

VPN

с поддержкой RADIUS-
протокола

ActiveSync

VDI

Outlook

(веб. версия)

WinLogon

1C/Bitrix

**Работа по
протоколам**

OpenID Connect,
OAuth 2.0, ADFS,
Radius, LDAP,
SAML, ActiveSync.

В перспективе: Linux, On-prem

Контур ID

Возможности Контур.ID

Способы подтверждения 2ФА

PUSH-уведомления



Подтвердите вход

сейчас

В сервисы Контура как
m.ivanova@pochta.ru

OTP-коды

Ключ выдан пользователю
ivanov@kontur.ru

KONTUR.RU ivanov@kontur.ru

947 583

Звонки

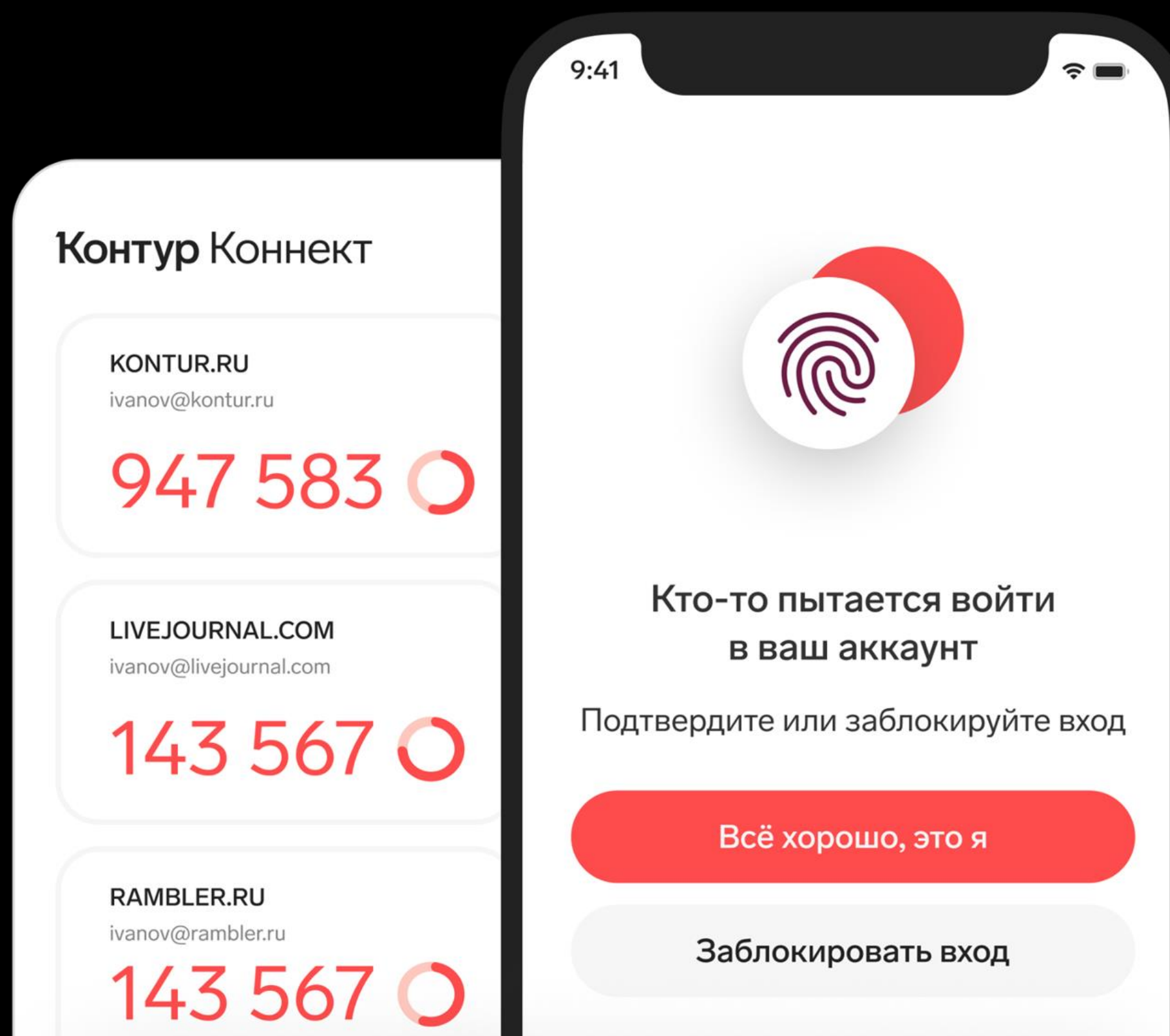


Примите звонок

Сейчас вам поступит текстовый
звонок. Ответьте на него, чтобы
подтвердить вход.

Возможности Контур.ID

Мы разработали собственное приложение Контур.Коннект с удобным интерфейсом для подтверждения второго фактора



Возможности Контур.ID

- Синхронизация пользователей с AD (Active Directory)
- Возможность выделить группы сотрудников для подключения второго фактора
- API Контур.ID
- Система Контур.ID поддерживает масштабирование посредством увеличения виртуальных ресурсов без пересмотра архитектуры системы (для возможности увеличения количества пользователей)

Контур.Доступ

Безопасное администрирование
удаленных пользователей



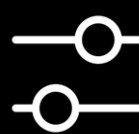
Контур Доступ

kontur.ru/dostup

Возможности Контур.Доступ



Двухфакторная аутентификация, запрет анонимных подключений, TLS-шифрование и защита от брутфорса



Возможность контролировать соединение на стороне абонента, возможность настроить запрос на разрешение подключения к компьютеру абонента



Кроссплатформенность (поддержка подключений с компьютеров и устройств на любой ОС, где есть браузер, к компьютерам на Windows, Linux и macOS) и серверная версия



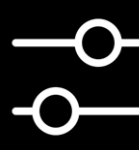
Группировка контактов по папкам и назначение прав доступа ИТ-специалистов к ним, журналирование подключений

Контур Доступ

Возможности Контур.Доступ



Возможность направления трафика P2P



Включен в Реестр российского ПО, имеет аттестат соответствия требованиям приказа ФСТЭК России N°21 для 3 уровня защищенности персональных данных



Собственный код, участие в программе bugbounty standoff365



Настройка групп доступа для обеспечения разного уровня тех. поддержки

Контур Доступ

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



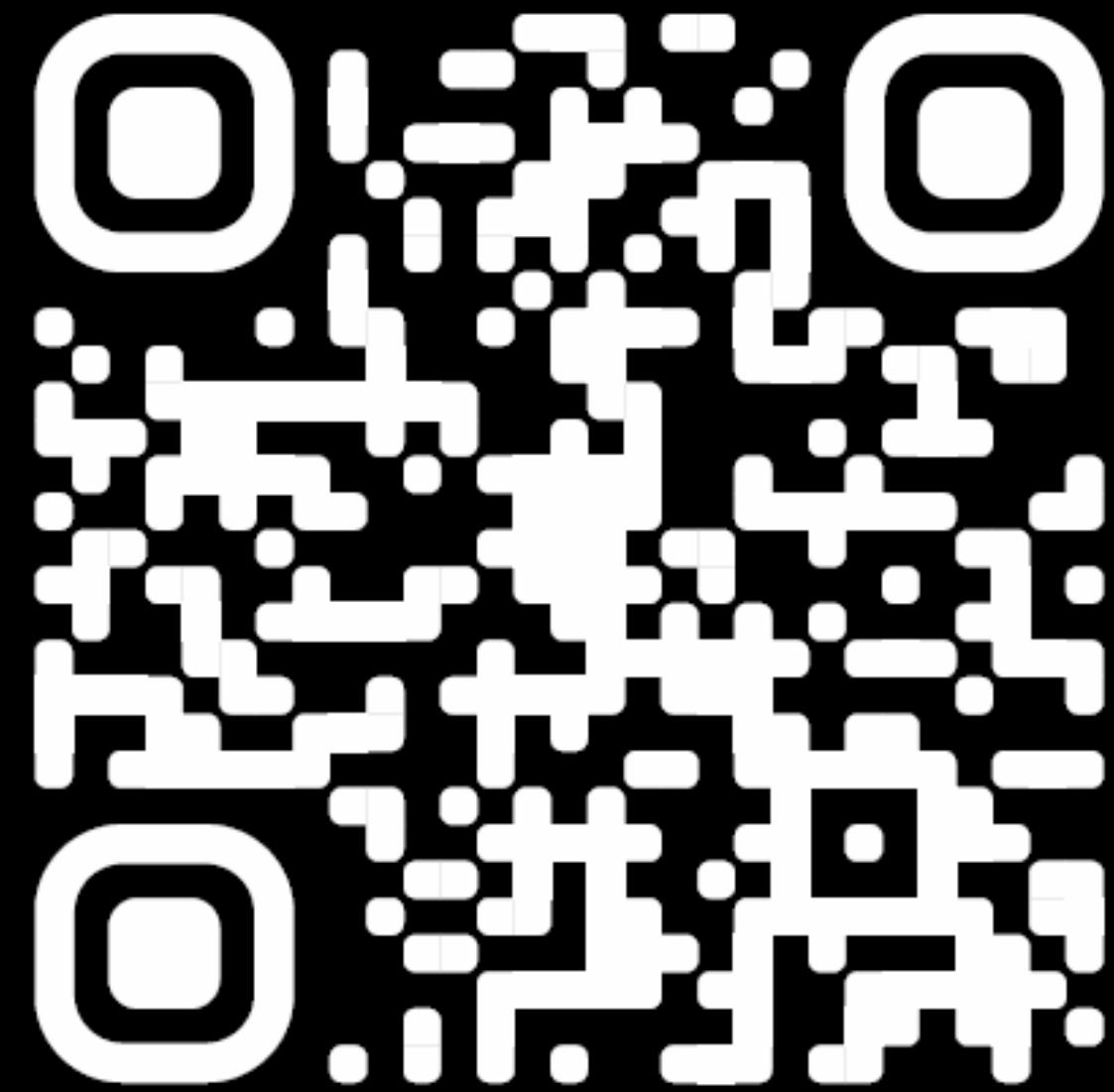
Сервис для системных
администраторов

Защита критических
точек инфраструктуры



Сервис
привилегированных
пользователей

**Узнать больше и оставить
заявку на тестирование
продуктов ИБ**



**Спасибо
за внимание!
Есть вопросы?**



Контур