Современные подходы к кибербезопасности

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

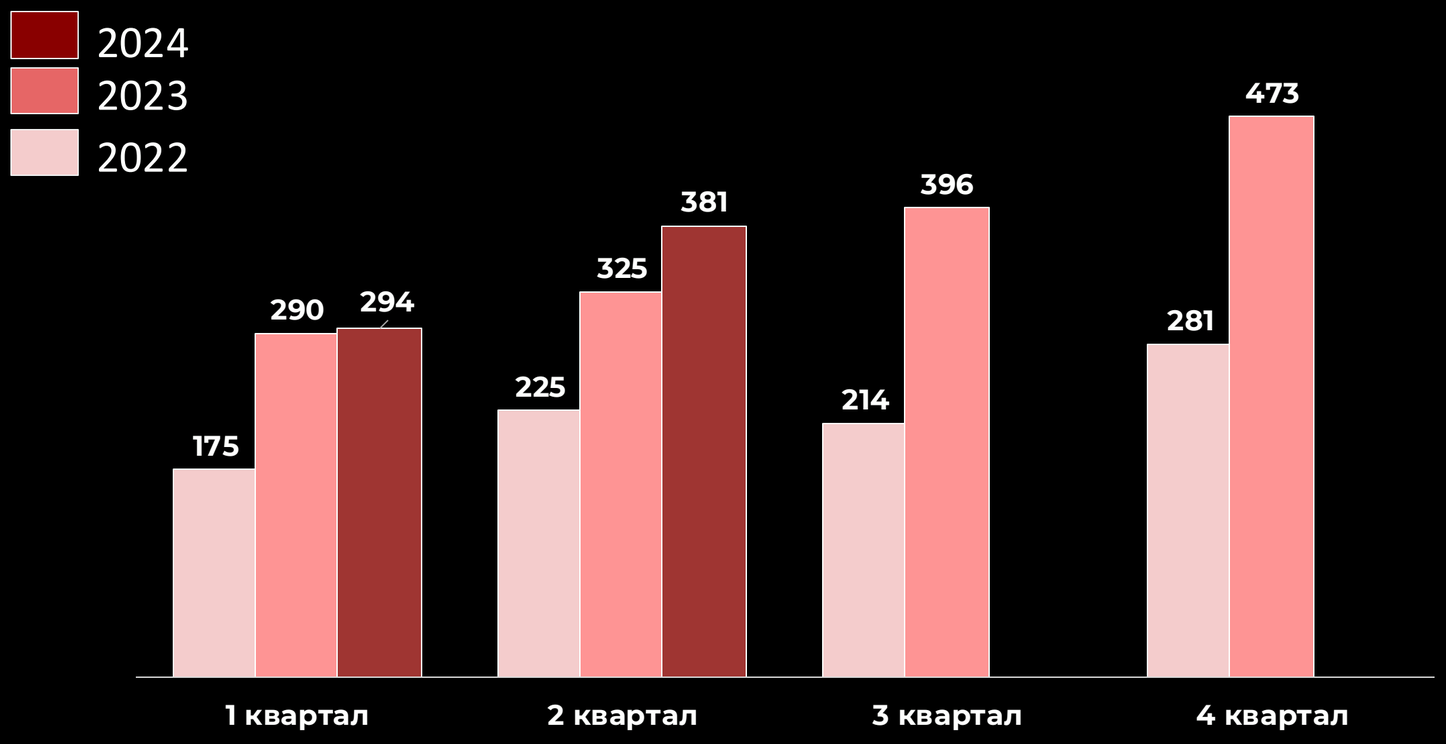
>80%

утечек информации произошли в результате кибератак

По данным аналитического отчета InfoWatch 2023 г. по РФ

События информационной безопасности в РФ

Распределение событий ИБ
по кварталам, тыс.



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

В 1-2 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

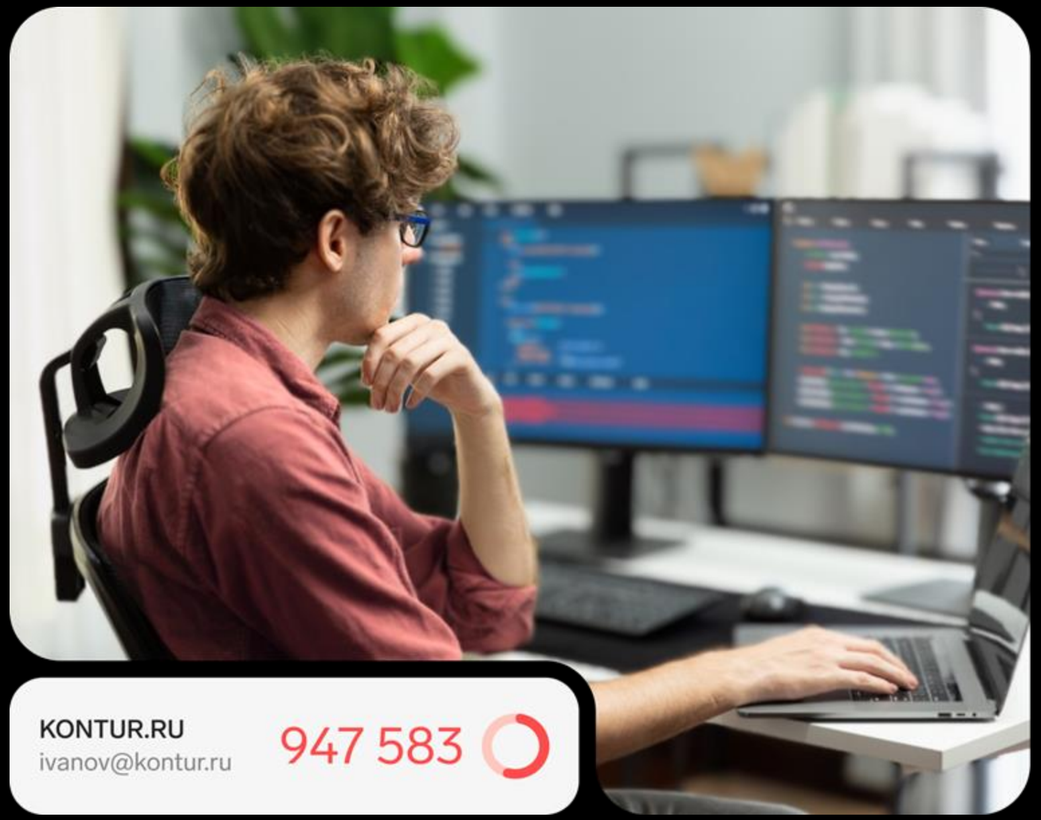
1 место
среди SaaS-поставщиков России по объему выручки по итогам исследования CNews Analytics: Крупнейшие поставщики услуг SaaS 2022 года

>5 000
клиентов курируют безопасность компаний благодаря сервисам Контура

>250 000
сотрудников компаний-клиентов пользуются сервисами ИБ

Контур.ID — двухфакторная аутентификация

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



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.

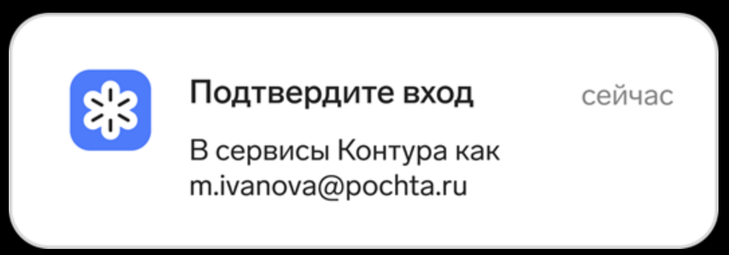
В перспективе: Linux, On-prem

Контур ID

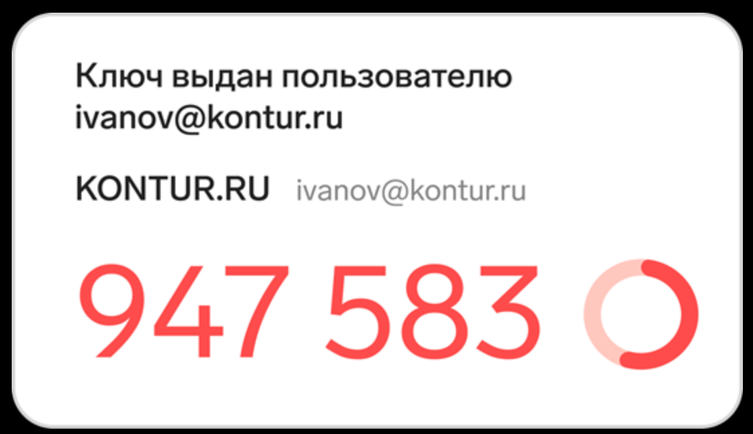
Возможности Контур.ID

Способы подтверждения 2ФА

PUSH-уведомления



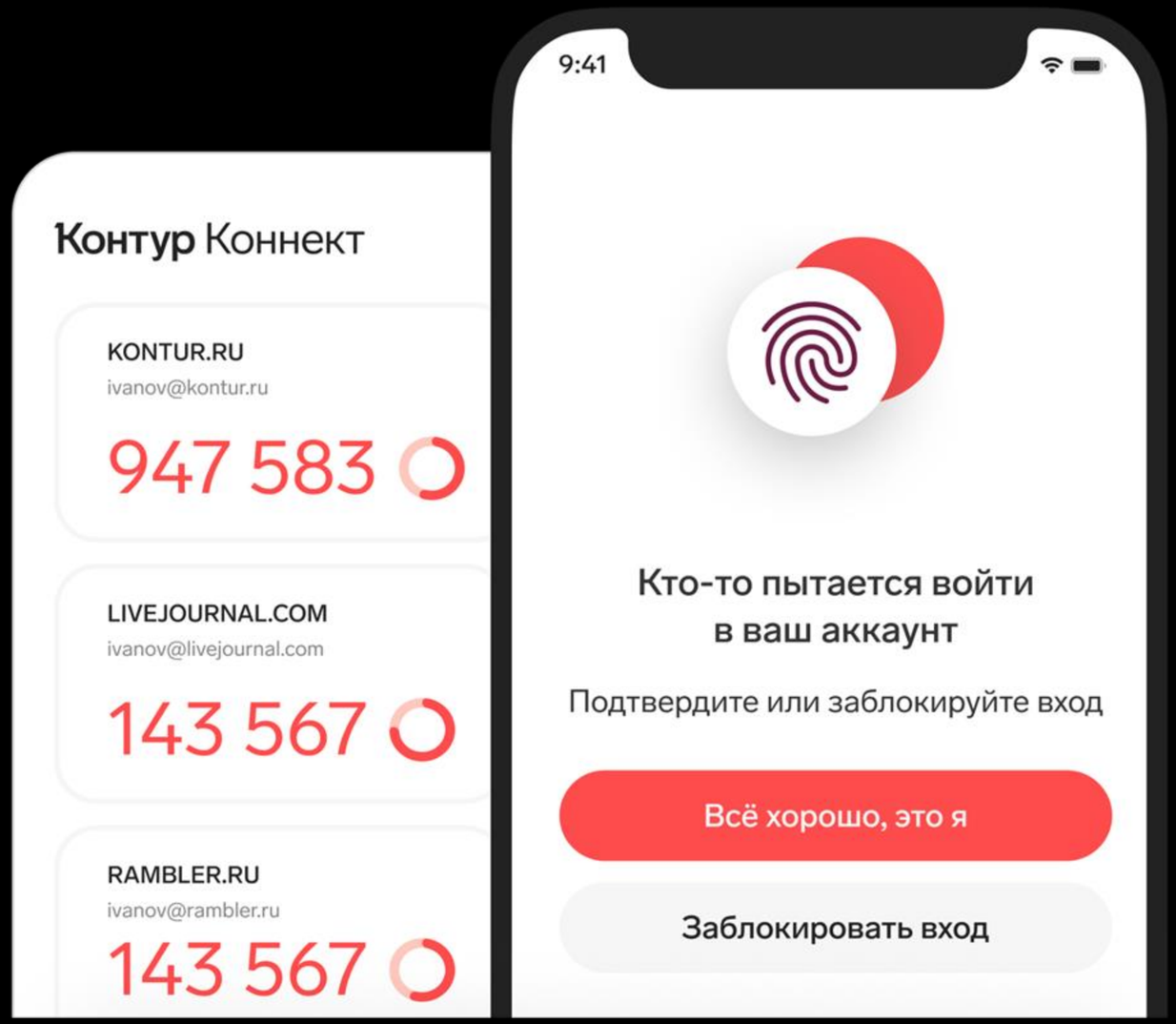
OTP-коды



Звонки

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)

Кейс: паразитирование в почте

От кого: Отдел информационной беССопасности
Кому: Алексею

Если вы получили это письмо, значит Отдел информационной безопасности компании смог подобрать ваш доменный пароль — нужно сменить его на более сложный.

Для изменения пароля необходимо перейти по ссылке и ввести данные своей учетной записи.

Если вы не смените пароль, вашу учетную запись заблокируют. Разблокировать ее можно только через заявку от руководителя.

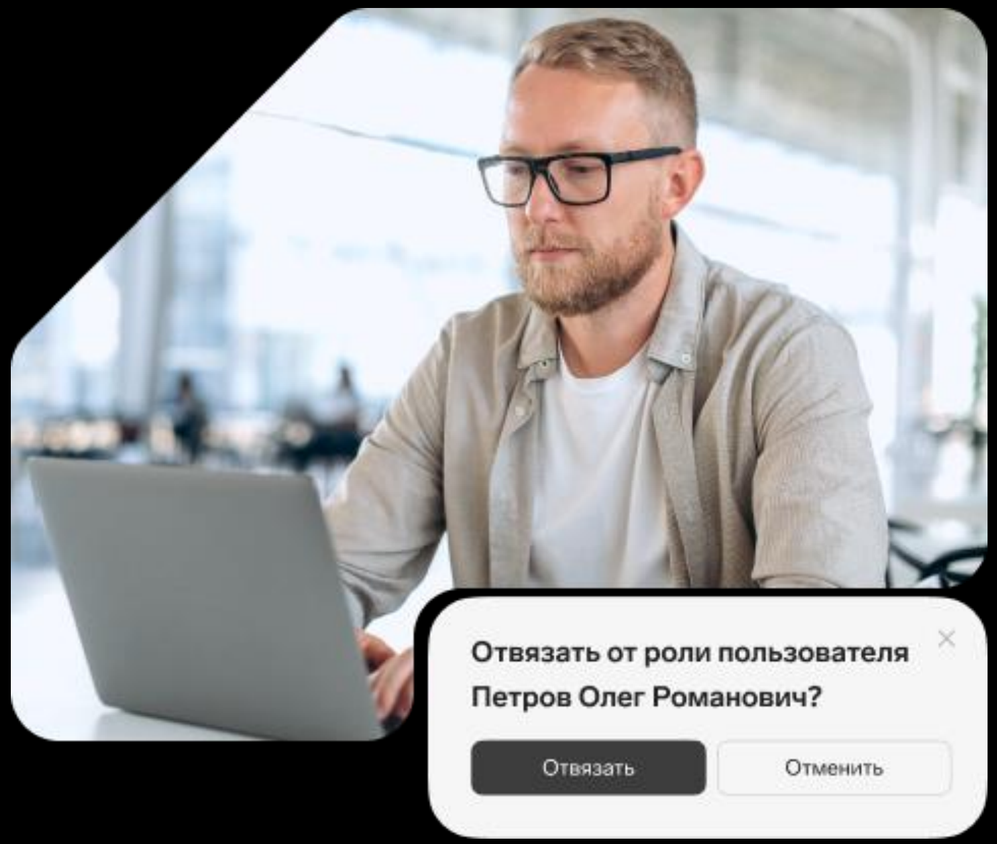
С уважением,
Отдел информационной безопасности

РЕШЕНИЕ:

Подключить на почту двухфакторную аутентификацию, чтобы никто просто так не смог подключится к ящику

Контур.РАМ

Система, которая защищает критически важные ресурсы вашей организации. Организует полный контроль и прозрачность действий привилегированных пользователей



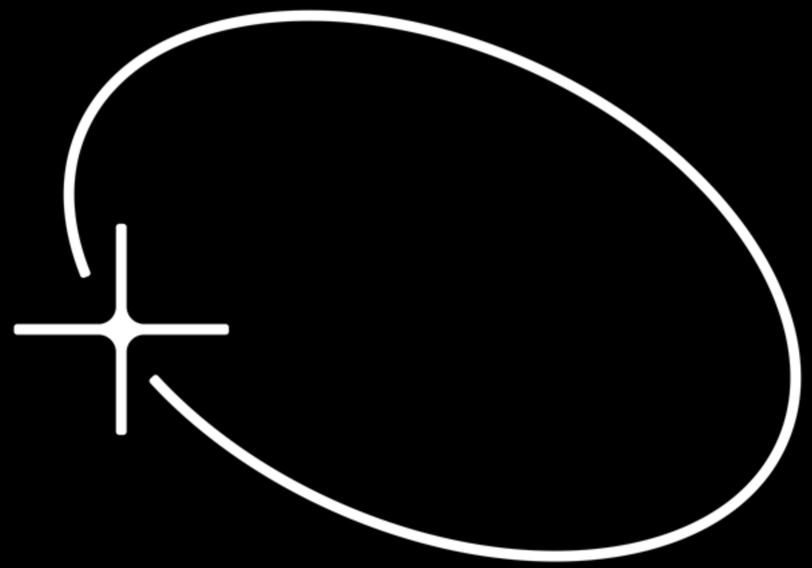
Контур РАМ

kontur.ru/lp/pam

Контур.PAM

Система предназначена для решения ключевых проблем, с которыми сталкиваются организации при управлении привилегированным доступом

Базовые сценарии: выдача доступов по RDP, мониторинг сессий внутри ресурсов.



Возможности Контур.PAM

1 Централизованное управление привилегированными учетными записями и правами доступа

2 Контроль доступа к приложениям и ресурсам, с помощью протоколов RDP

3 Веб интерфейс для просмотра текстового лога сессии удаленного доступа

4 Интеграция с Active Directory

Контур.Доступ

Безопасное администрирование
удаленных пользователей

Контур Доступ

kontur.ru/dostup

Возможности Контур.Доступ

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

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

3 **Группировка контактов по папкам и назначение прав доступа ИТ-специалистов к ним, журнал событий**

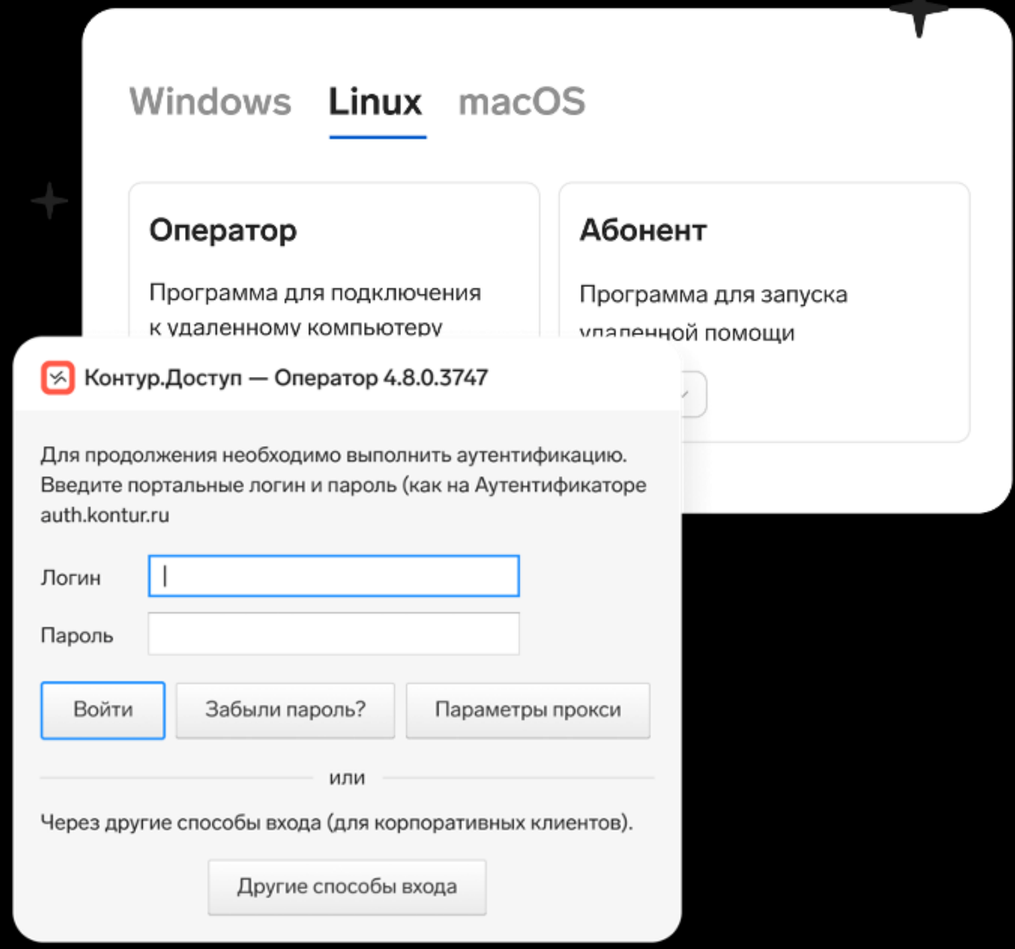
Контур Доступ

Возможности Контур.Доступ

4 **Разворачивание на серверах компании**

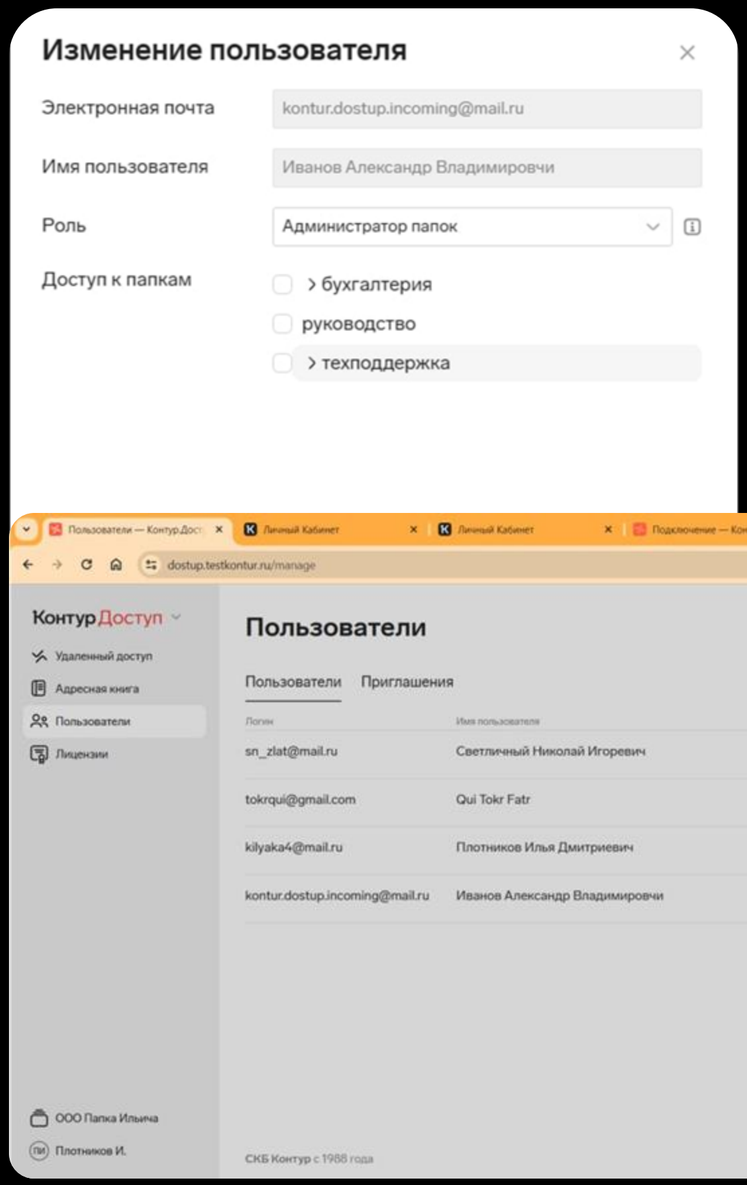
5 **Кроссплатформенность (поддержка подключений с компьютеров и устройств на любой ОС, где есть браузер, к компьютерам на Windows, Linux и macOS) и серверная версия**

6 **Персонализация (SSO, возможность настройки прокси-сервера)**



Контур Доступ

Возможности Контур.Доступ



7 **Управление пользователями-операторами через личный кабинет, назначение ролей, выдача прав доступа**
Командная строка, Wake-On-Lan

Контур Доступ

Возможности Контур.Доступ

Возможность направления трафика P2P

Включен в Реестр российского ПО, имеет аттестат соответствия требованиям приказа ФСТЭК России №21 для 3 уровня защищенности персональных данных

Собственный код, участие в программе bugbounty standoff365

Контур Доступ

Кейс

Потребности

- **Работа как в локальной сети так и с не доменными машинами**
- **Внутренняя аутентификация с действующими учётными записями**
- **Возможность быстрой отправки дистрибутива сотруднику**
- **Передача данных без ограничений**

UEM

Система унифицированного управления конечными устройствами: первый модуль - сбор информации о конфигурации и составе программного обеспечения управляемых устройств

Контур Доступ

kontur.ru/dostup

Текущие возможности UEM

Инвентаризация - система сбора, хранения и мониторинга информации о парке устройств с интерфейсом для системного администрирования (железо и ПО)

Контур Доступ

Будущие возможности UEM

Настройка рабочих мест по шаблонам – сервис удобно и просто настроит компьютер по заданному шаблону под роль или задачу (силами самого сотрудника или сисадмина), а также позволит поддерживать компьютер в актуальном состоянии

Удаленная настройка компьютеров. Система поддерживает удаленную конфигурацию устройств, что позволяет вносить изменения массово или точечно

Контур Доступ

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

staffcop®

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

staffcop®

Как работает staffcop?

Сбор данных

Агент собирает все события
о действиях пользователя
и движений 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®

staffcop

Кейс: Параллельный бизнес

Проблема:

В компании наблюдается значительное снижение продуктивности у одного из ключевых сотрудников за последние несколько месяцев. Это понижение продуктивности началось неожиданно и продолжается, несмотря на предыдущие высокие показатели и активное участие сотрудника в работе.

Подозреваемый:

Опытный сотрудник компании

Инцидент:

Подключался к удаленному компьютеру у себя дома. Параллельно занимался делами своего ЮЛ

Какой функционал Staffcop помог разобраться в данной ситуации?

Функционал Staffcop для расследования:

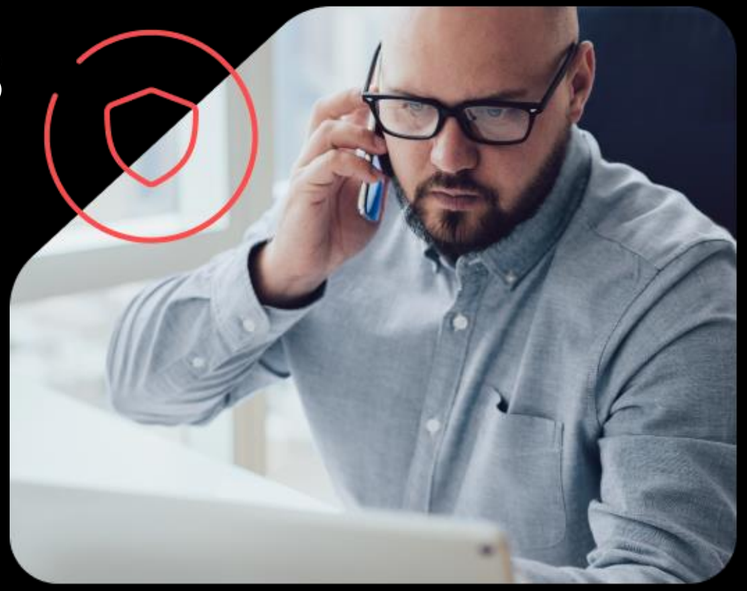
- Время активности
- Снимки экрана

ИТОГ

- Увидели постоянную активность программы для подключения к удаленному компьютеру
- Проанализировали скриншоты
- Сотрудник переведен на полставки

Формула защиты от киберугроз

Комплекс решений Контура для информационной безопасности компании



Узнать больше и оставить заявку на тестирование продуктов ИБ

Спасибо
за внимание!
Есть вопросы?

Контур