Защита учетных записей сотрудников

Дмитрий Мельников

Менеджер проектов
по внедрению Контур.ID

Контур — один из крупнейших разработчиков ПО в России

35 лет на рынке

Создаем решения для индивидуальных предпринимателей и крупных корпораций

Больше 70 продуктов для бизнеса

В том числе Диадок, Экстерн, Бухгалтерия и Фокус

1 место

SaaS в России по данным CNews

2.2 млн

Клиентов в России и за рубежом

Контур – это безопасность.

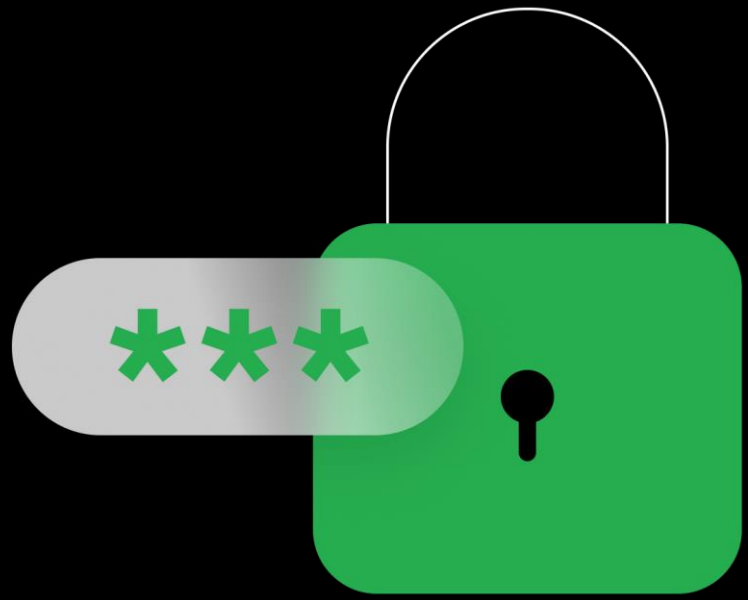
В группу компаний КОНТУР вошло ООО АТОМ БЕЗОПАСНОСТЬ из Новосибирска.

Флагманский продукт компании — платформа Staffcop, которая предотвращает утечку данных с рабочих компьютеров.

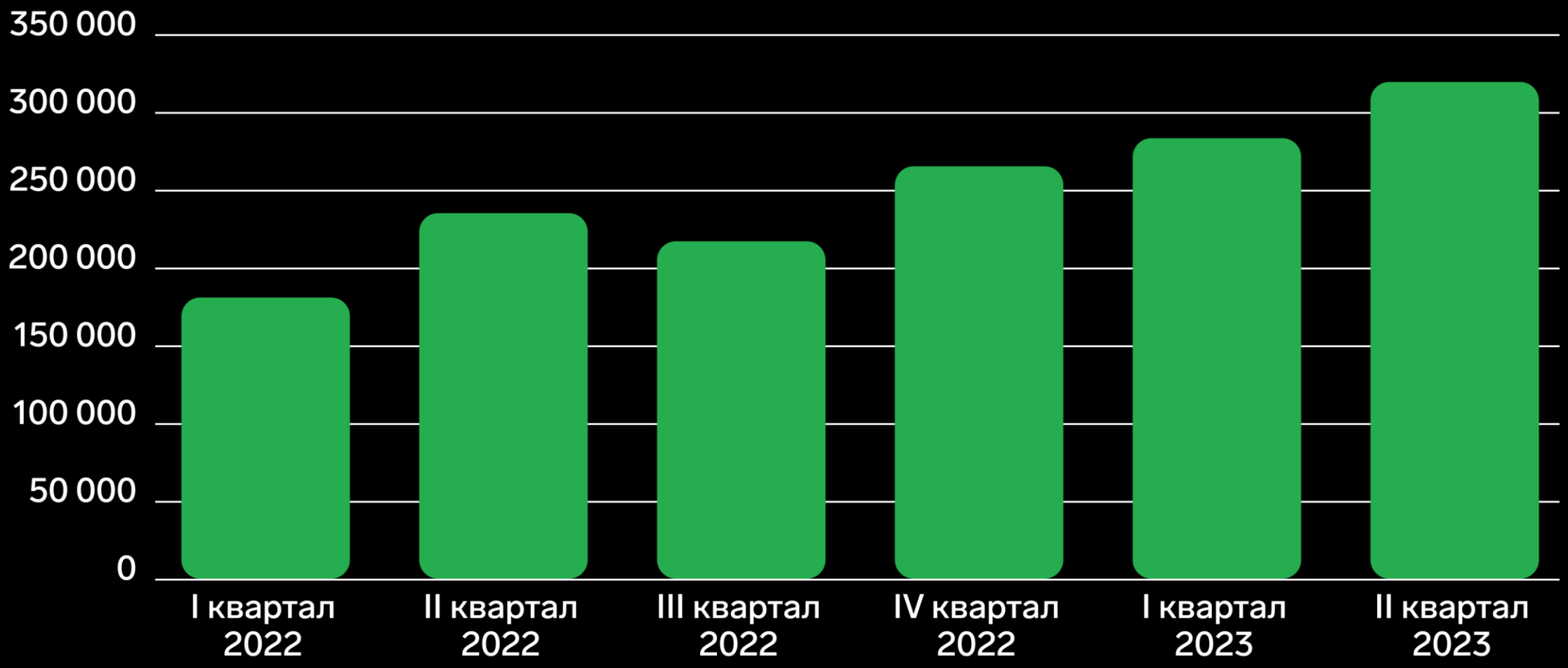
Благодаря этой покупке Контур вышел на рынок информационной безопасности.

Проблематика кибербезопасности

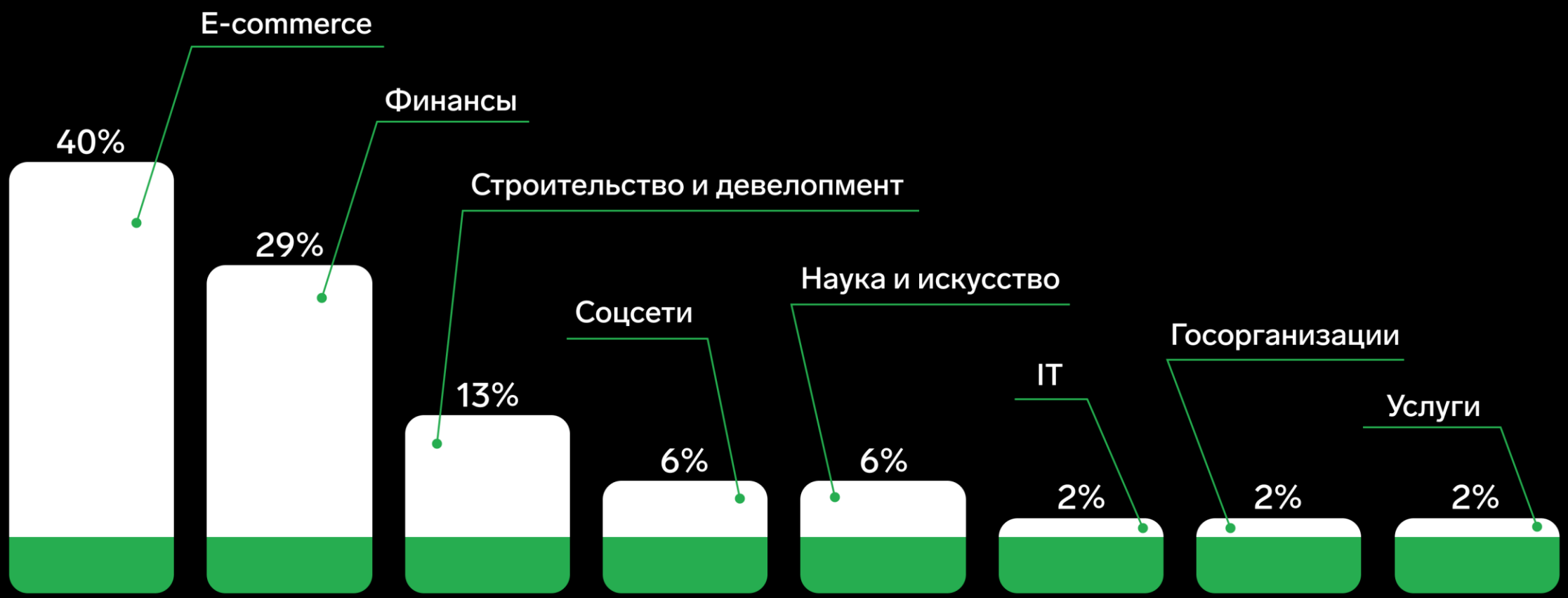
- Фишинг
- Вредоносное ПО
- DDos



Распределение событий ИБ по кварталам



Распределение утечек по отраслям



Статистика по атакам

Распределение ИБ-инцидентов в четвертом квартале 2022 года по категориям

*Несанкционированный доступ к информационным системам и сервисам.

Источник: «Ростелеком Солар»

Причины инцидентов

- **Простые пароли**

  Многие сотрудники всё еще используют слабые пароли, которые легко поддаются взлому. Это может создать уязвимость в защите учетных записей.

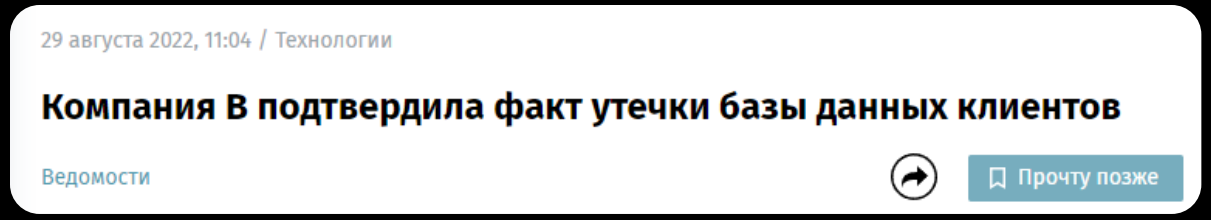
- **Отсутствие многофакторной аутентификации**

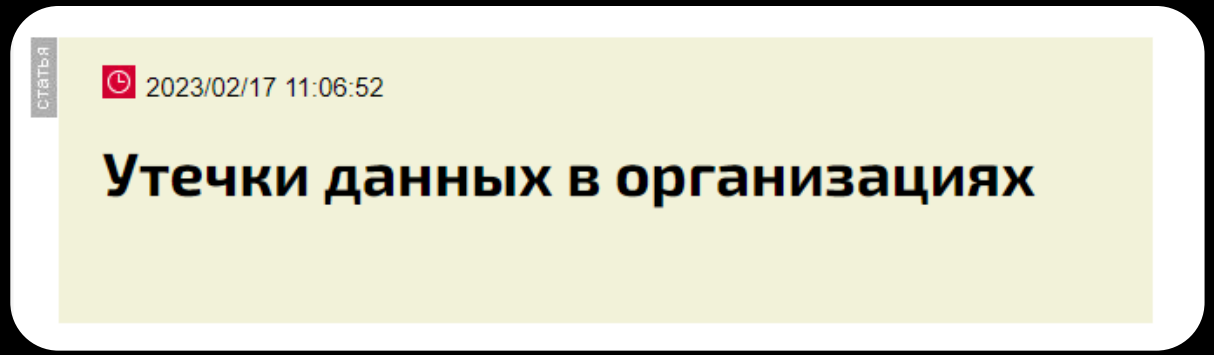
  Использование только пароля не является надежным методом защиты учетных записей сотрудников

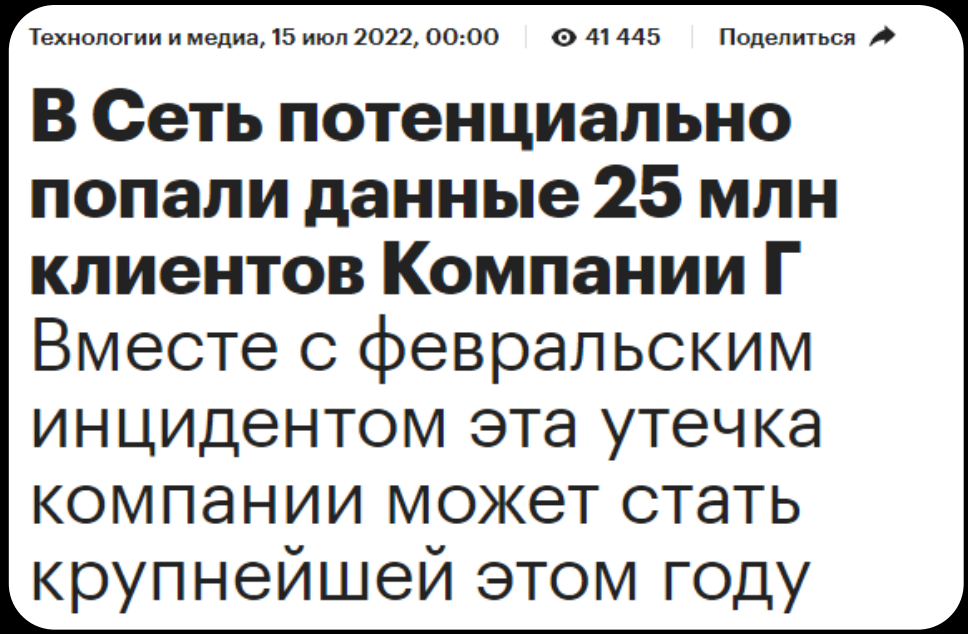
- **Недостаточное обновление программного обеспечения**

  Не обновлённые программы и операционные системы могут содержать уязвимости, которые могут быть использованы для компрометации учетных записей сотрудников.

Новостные заголовки







Утечка данных.
Сервис доставки еды

Кейс № 1

В РОССИИ 16:28, 21 декабря 2022

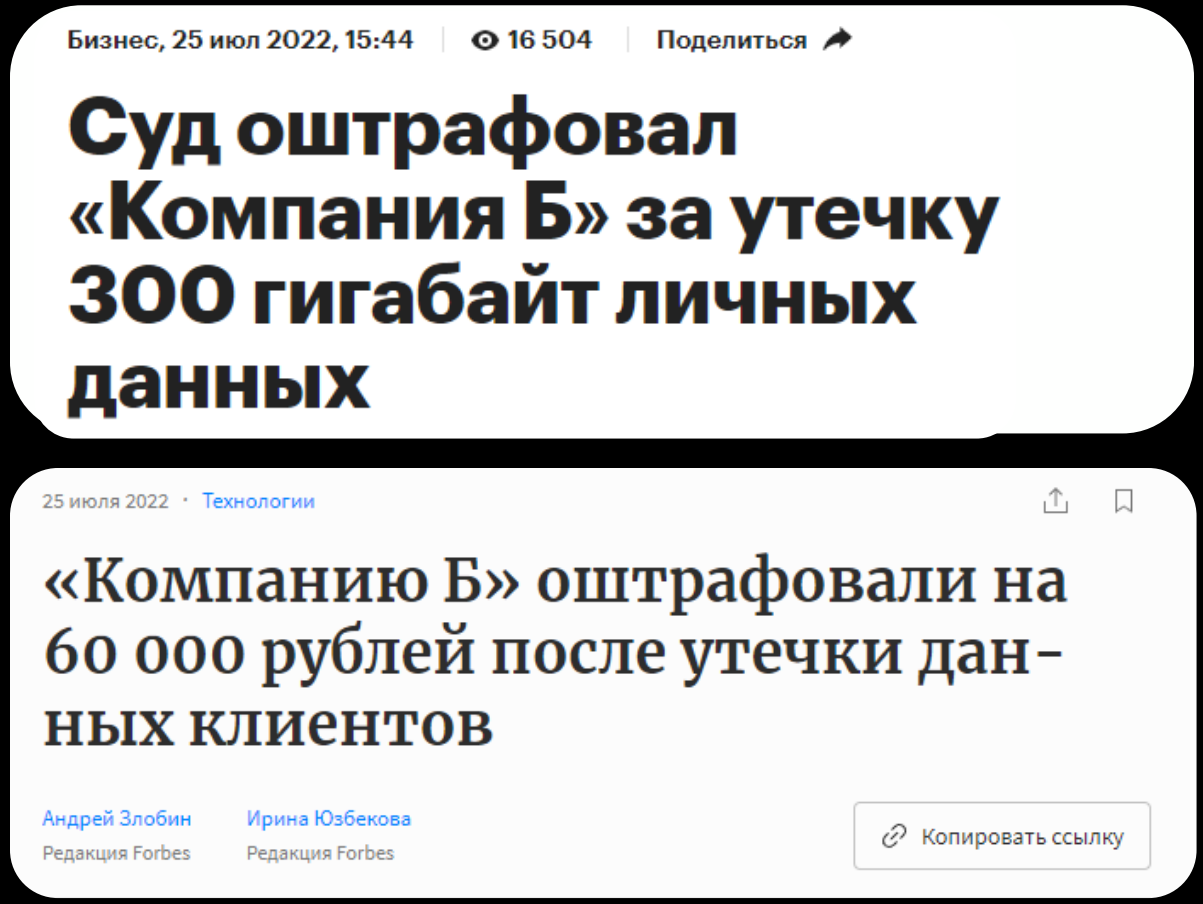
"Организация А" признана потерпевшей по делу об утечке данных клиентов

На сайте собраны данные пользователей, об утечке которых сама Организация А в интернет попали имена, номера телефонов, адреса и техническая информация об их заказах. В утечку не попали логины и пароли, а также данные банковских карт пользователей.

В компании объяснили, что инцидент произошел из-за недобросовестных действий одного из сотрудников. Клиенты, которых коснулась утечка, получили предупреждающие письма.

Утечка из медучреждений

Кейс № 2



Бизнес, 25 июл 2022, 15:44 | 16 504 | Поделиться

Суд оштрафовал «Компания Б» за утечку 300 гигабайт личных данных

25 июля 2022 · Технологии

«Компанию Б» оштрафовали на 60 000 рублей после утечки данных клиентов

Андрей Злобин
Редакция Forbes

Ирина Юзбекова
Редакция Forbes

Копировать ссылку

Пример инцидента

- Злоумышленник взломал компанию А, опубликовав данные о пользователях: ФИО, должность, телефоны, почты и т.д.
- В данной базе нашли интересного человека из компании Б.
- Поиск по номеру телефона из различных баз данных выдал более подробную информацию о сотруднике, личный и корпоративный email, а так хэш пароля.
- Поиск по личной почте или по телефону выдал слитые пароли от социальных сетей.
- Один из ранее утекших паролей отлично подошел к корпоративной учетной записи, что открывает доступ к чувствительной информации.

Последствия компрометации УЗ

Потеря лояльности со стороны клиентов или сотрудников

Финансовые потери: иски / штрафы, выкупы

Коммерческая тайна

Статистика по атакам

>50%

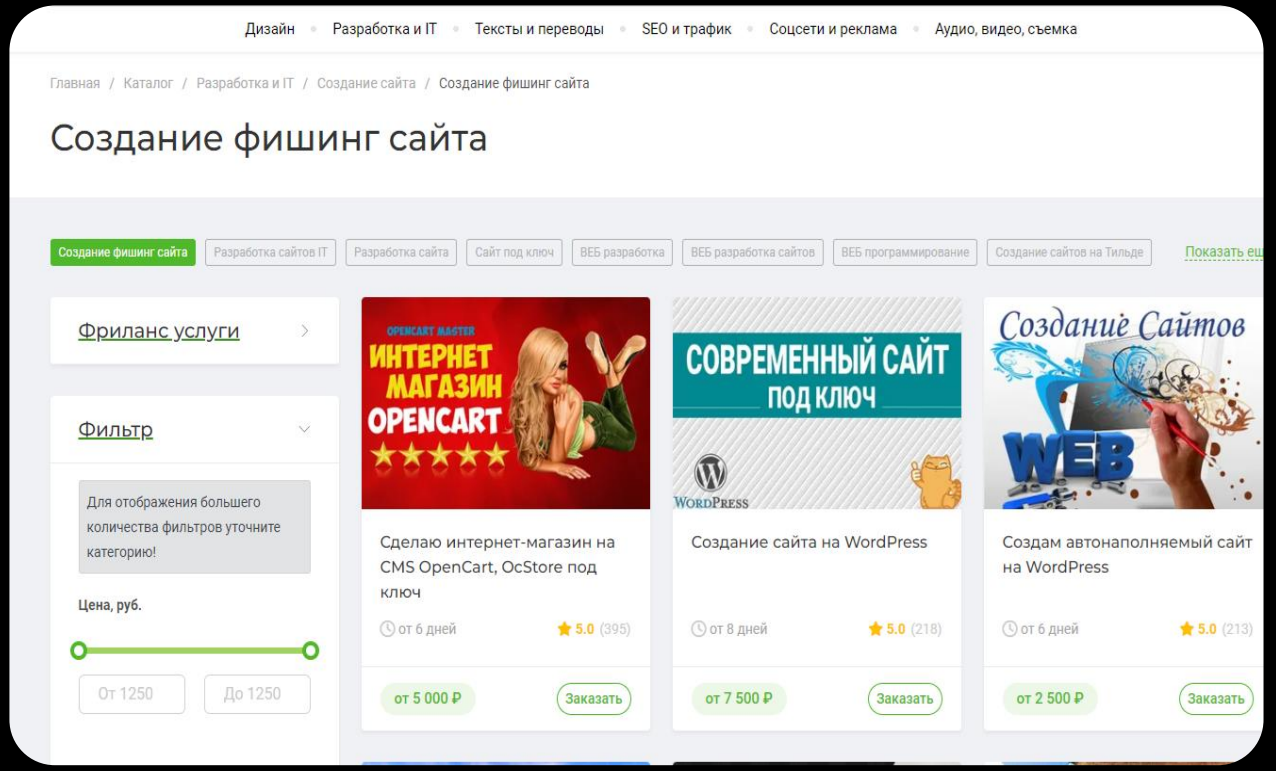
Более 50% атак по взлому аккаунтов приходится на фишинговые способы получения секретов

~10%

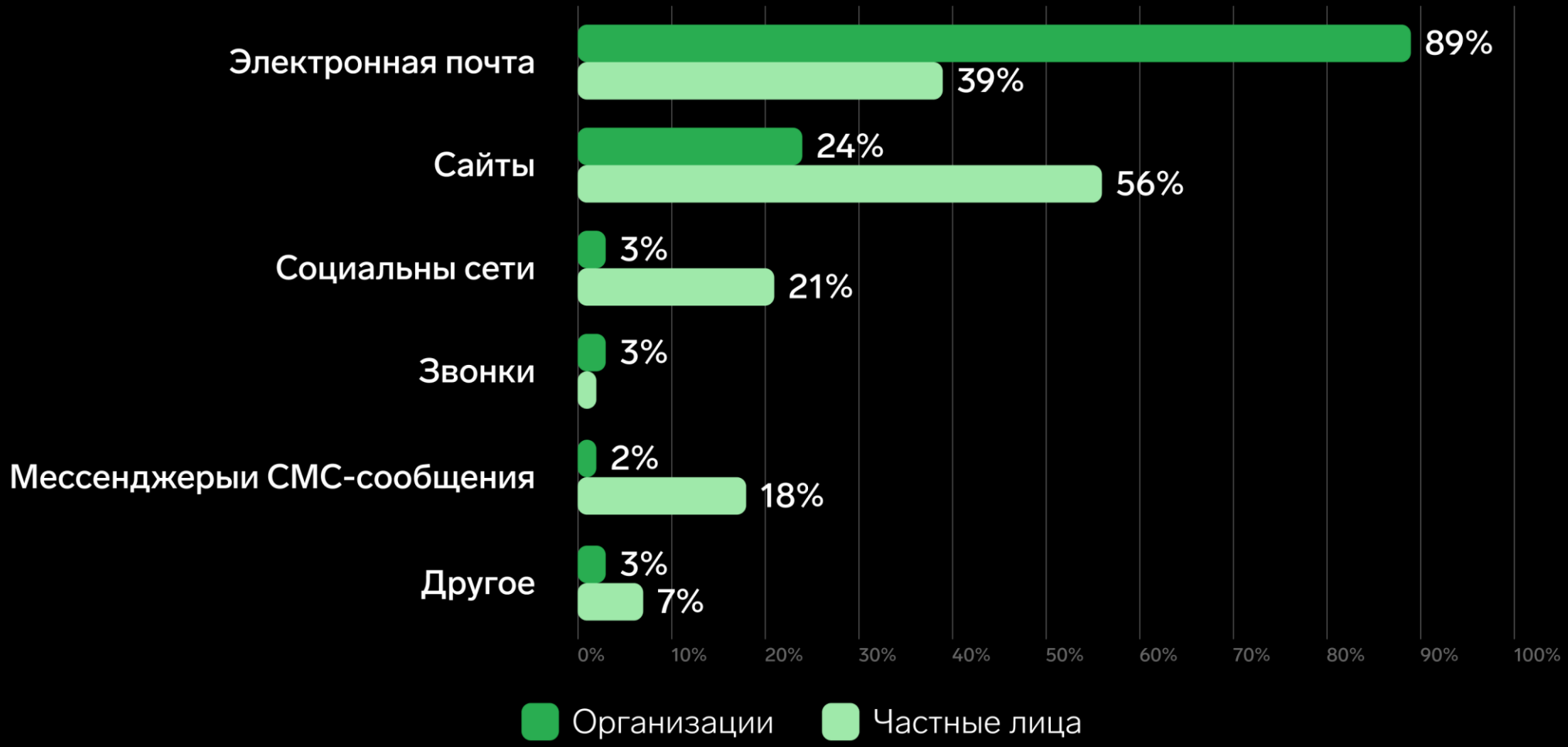
10% атак по взлому аккаунтов приходится на Brute-force атаки

Фишинг стал доступнее

Уже сформировался полноценный рынок — «Фишинг как услуга»
Phishing-as-a-Service -> PhaaS



Фишинг: каналы социальной инженерии



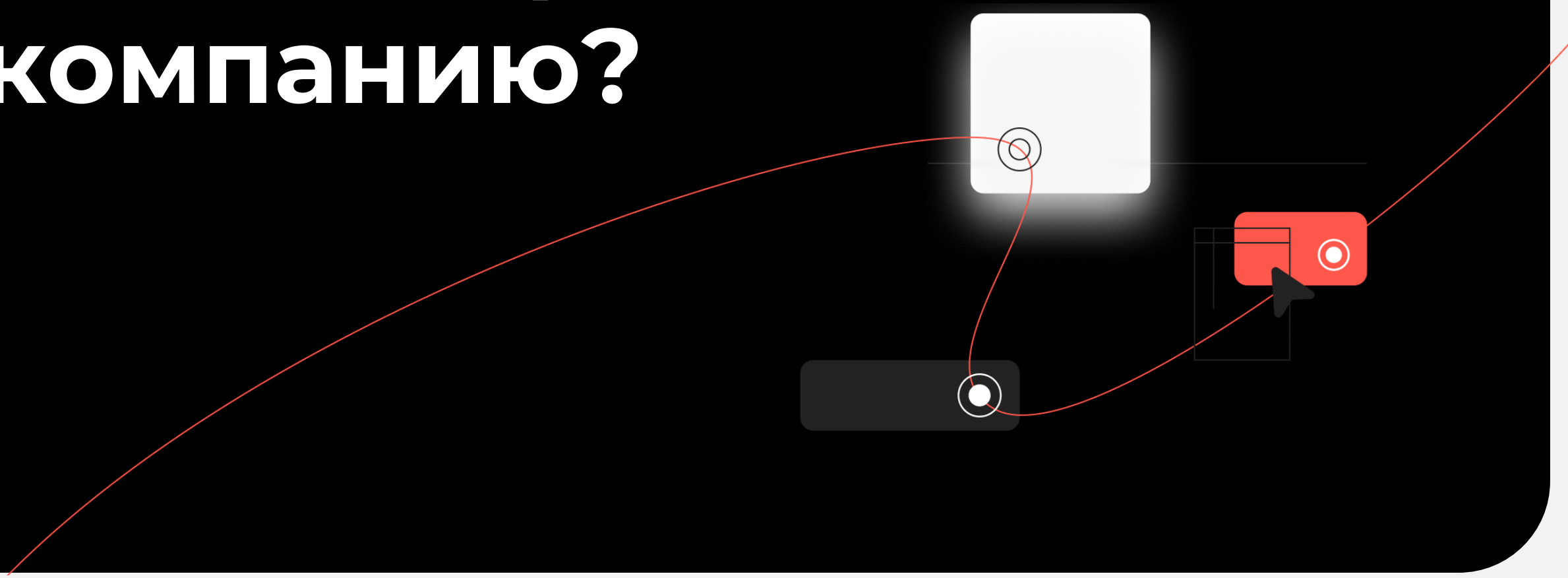
Brute-force атаки

- Банальный перебор паролей
- Перебор на основе базы часто встречаемых паролей
- Самое важное: Перебор по купленной базе паролей

Уязвимости в инфраструктуре:

- VPN
- Веб-сервисы, доступные из дикого интернета (Почта, ActiveSync)
- Отдельная защита критичных машин (RDP, SSH)

А как защитить компанию?



Контур

Двухфакторная аутентификация не спасает?

До 1% удачных случаев взлома аккаунта сопровождается взломом 2ФА

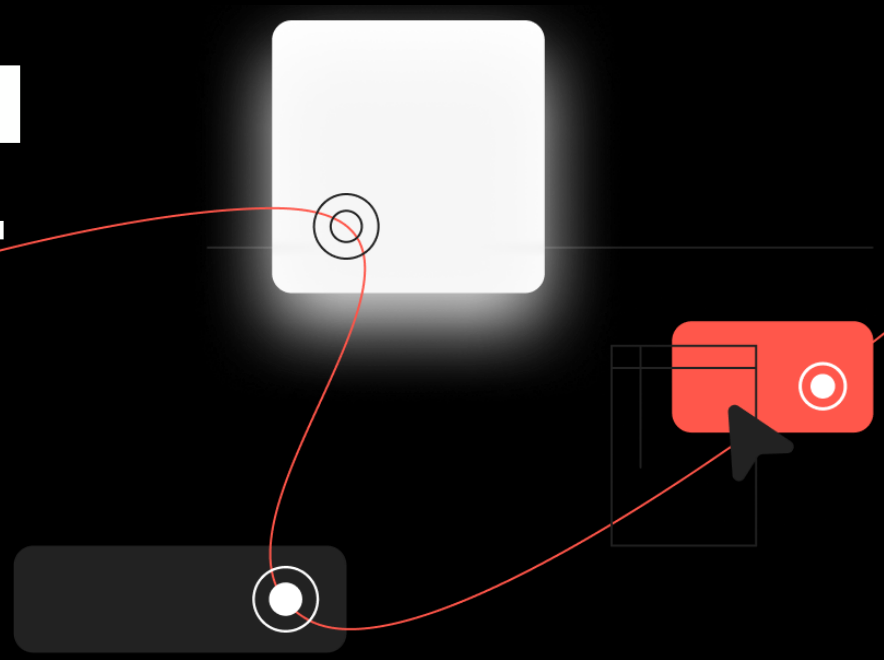
SMS небезопасны

Получение SMS основано на старом протоколе SS7, в котором есть архитектурные дыры.

Способы 2ФА:

- Звонки на номер телефона пользователя
- Сертификаты и Аппаратные ключи
- Push-уведомления
- Биометрия
- TOTP-коды

Контур.ID – защитит учетные записи сотрудников от взлома



Контур

Контур ID. Возможности

Сейчас

- VPN
- RDG
- OWA (IIS)
- ADFS
- ActiveSync

Скоро

- WinLogon
- Linux
- 1C\Bitrix
- SSH
- И другое

Контур ID в цифрах

>10000

внутренних пользователей, сотрудников компании Контур

~10000

внешних пользователей

99,99%

наше SLO

Панель управления Kontur.ID

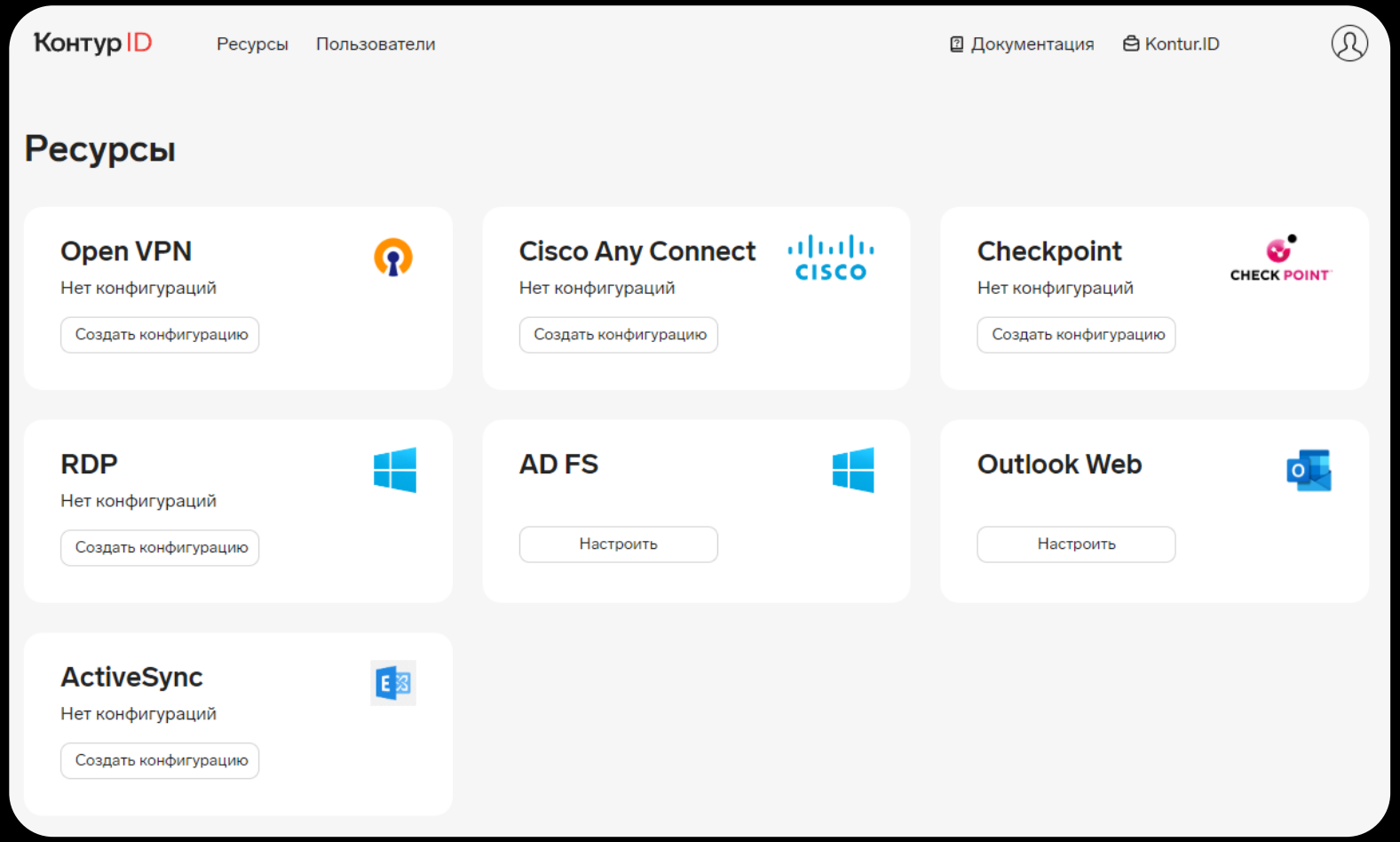


Схема 2ФА в VPN/RDP

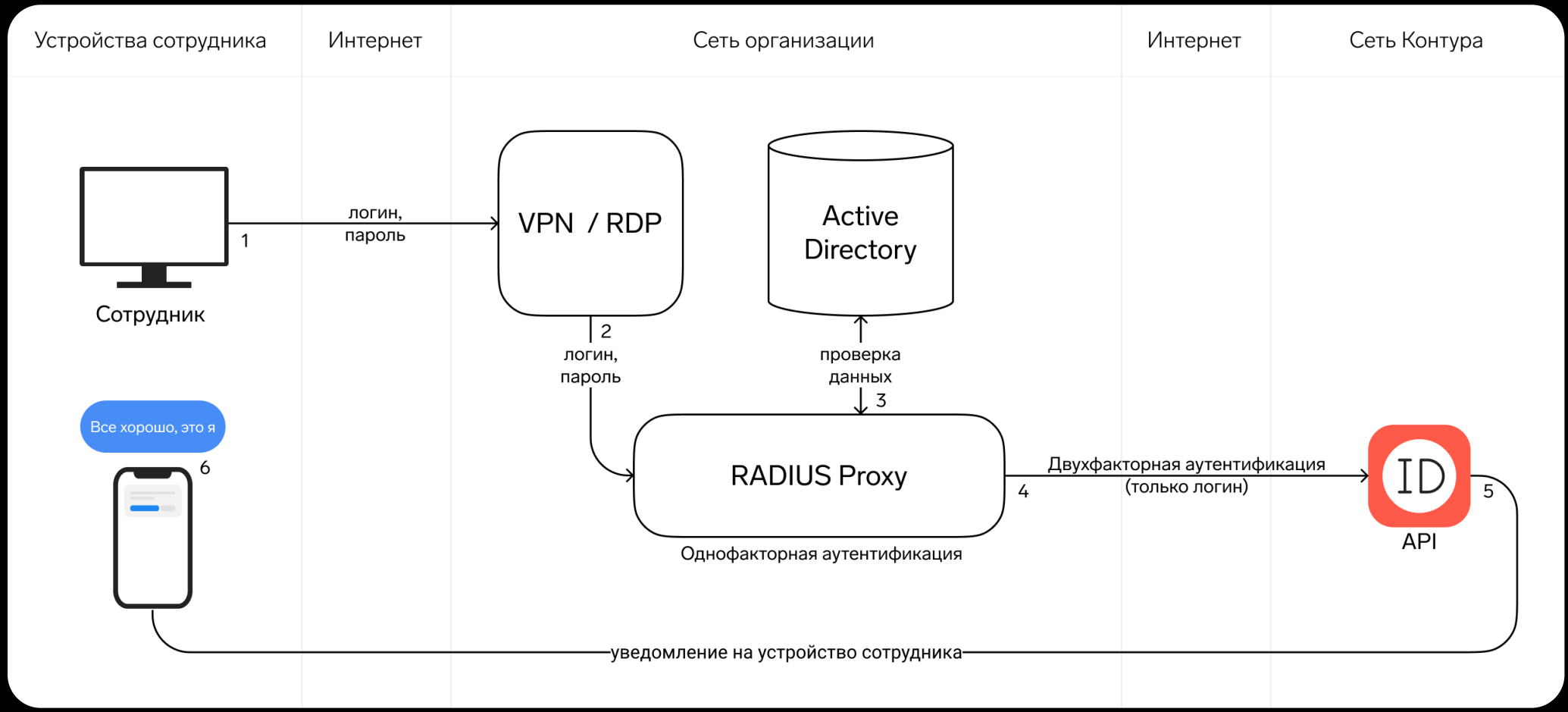
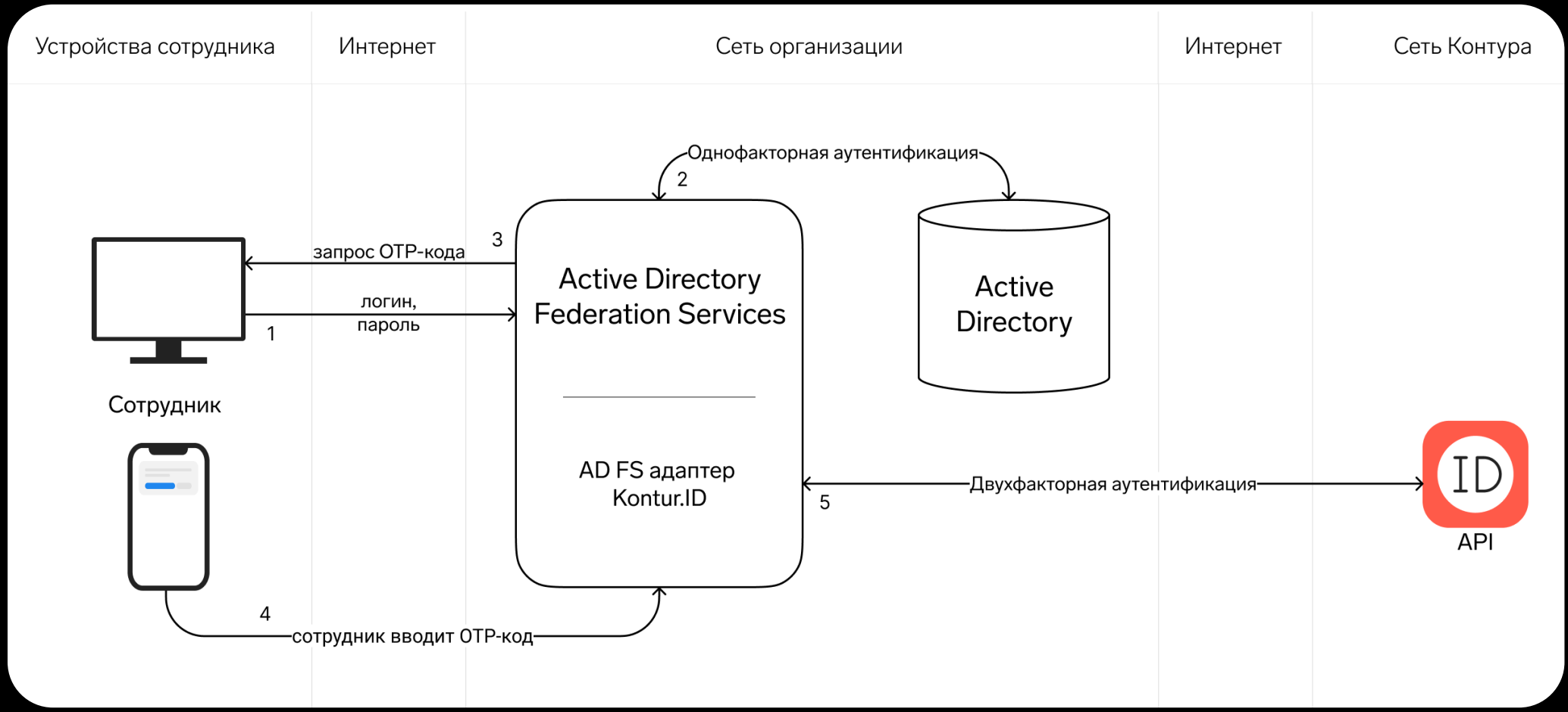
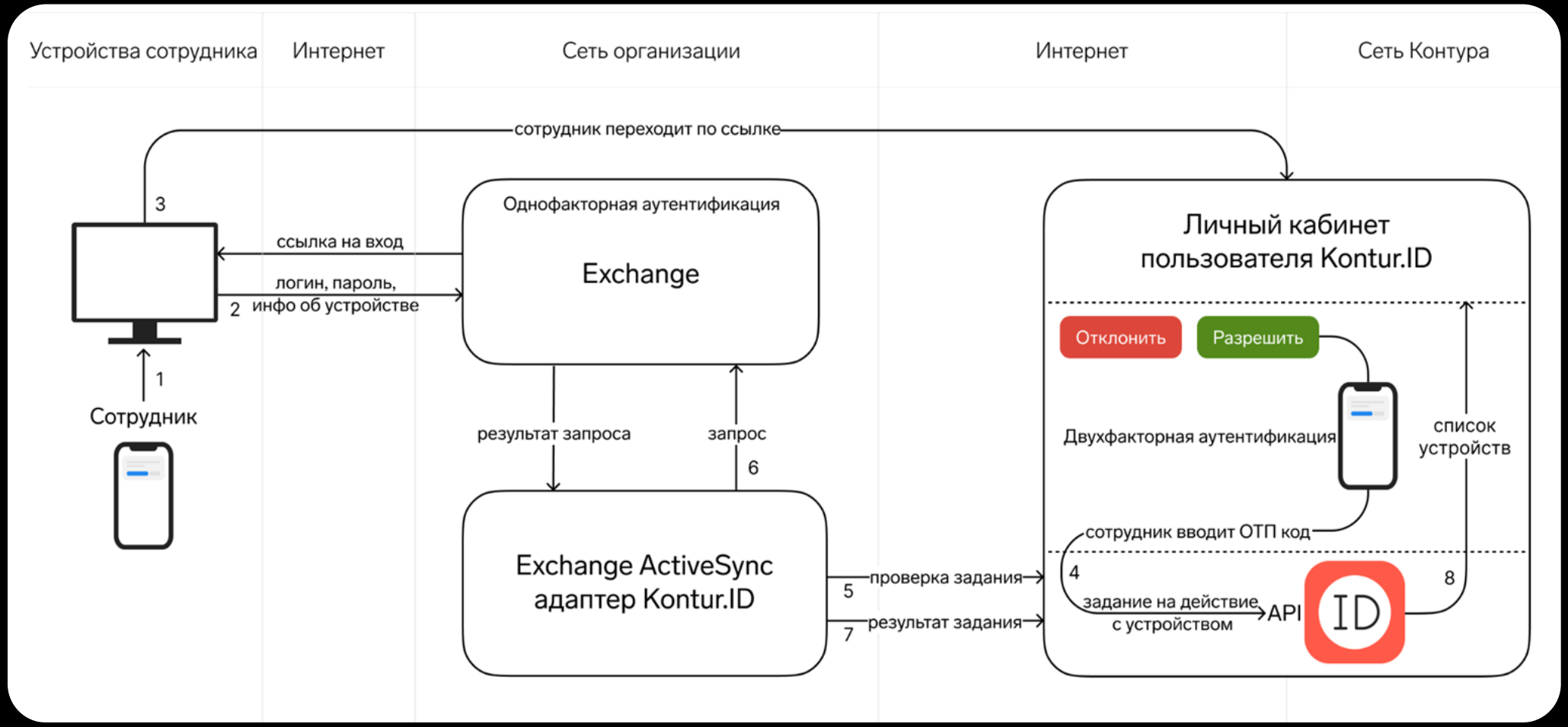


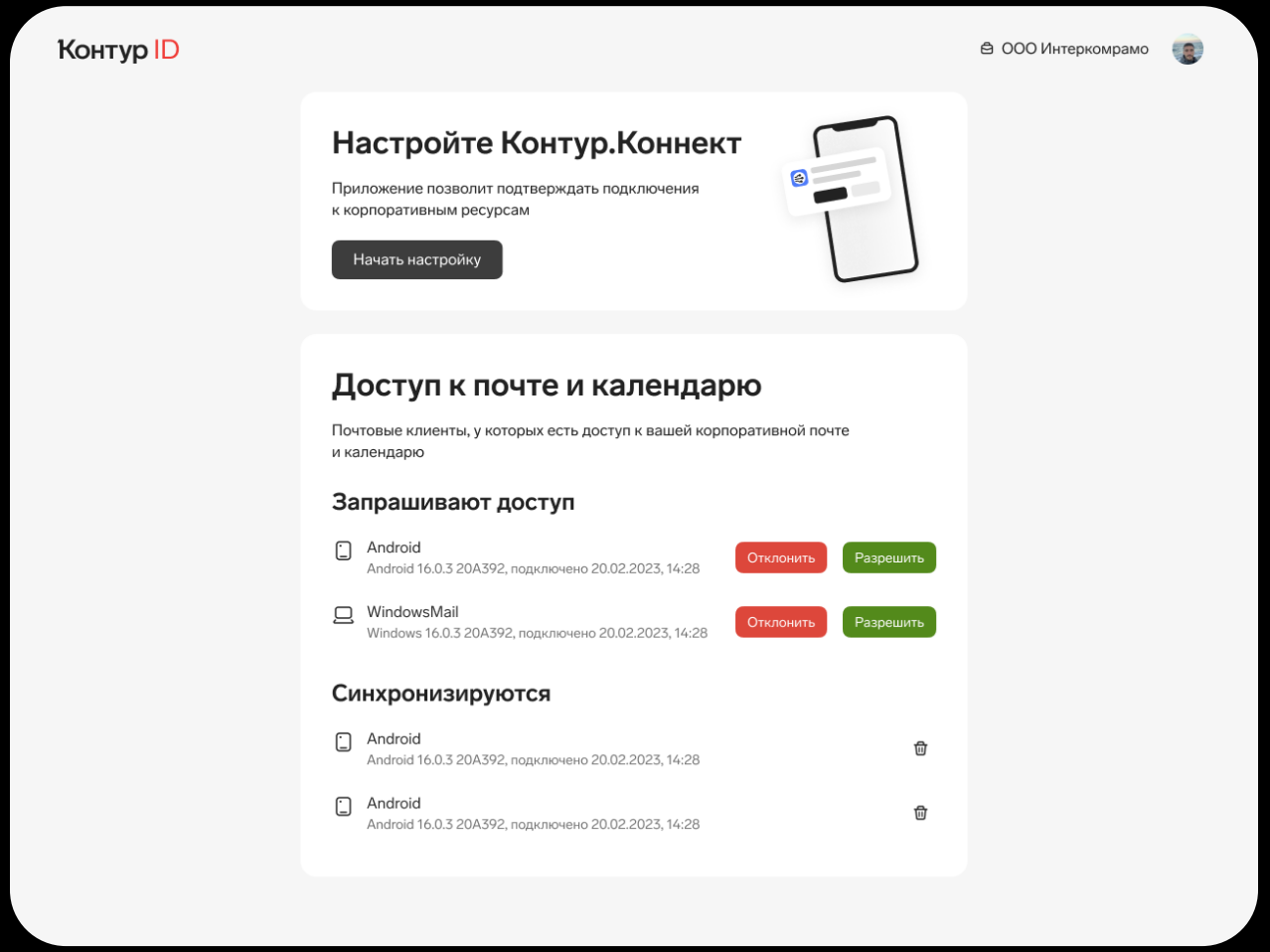
Схема 2ФА в ADFS

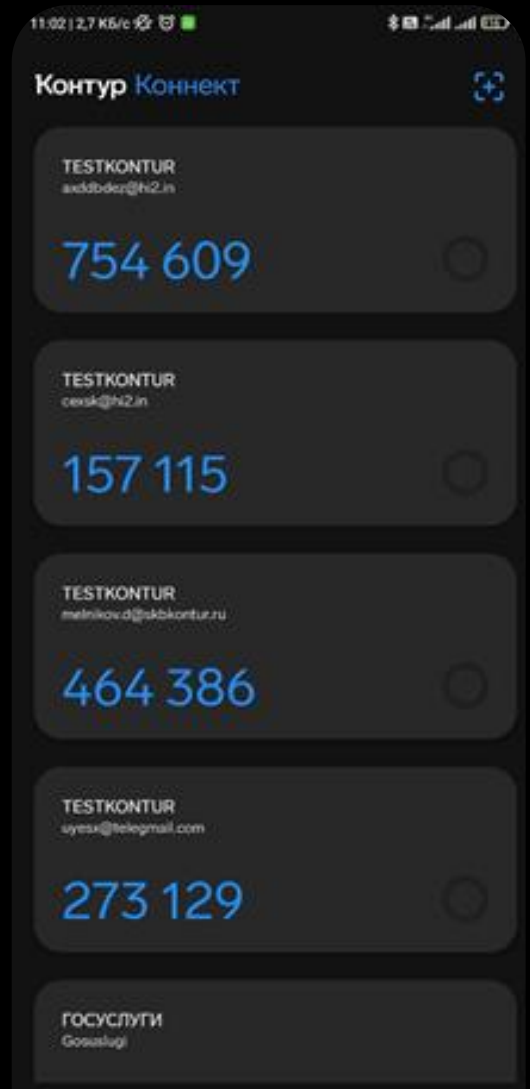


Exchange. ActiveSync



Личный кабинет и приложение





On-cloud

Простота и доступность

Экономия человеческих ресурсов на установку и поддержку.
Нет необходимости приобретать и обслуживать дополнительные сервера.

Безопасно

Аттестованные сервера
Находятся в России

Удобства

Сопровождение отделом внедрения и наличие технической поддержки

On-premise

Реализация «коробки»

в планах на конец 2024 года

DMZ

как альтернатива

Спасибо за внимание!

Дмитрий Мельников