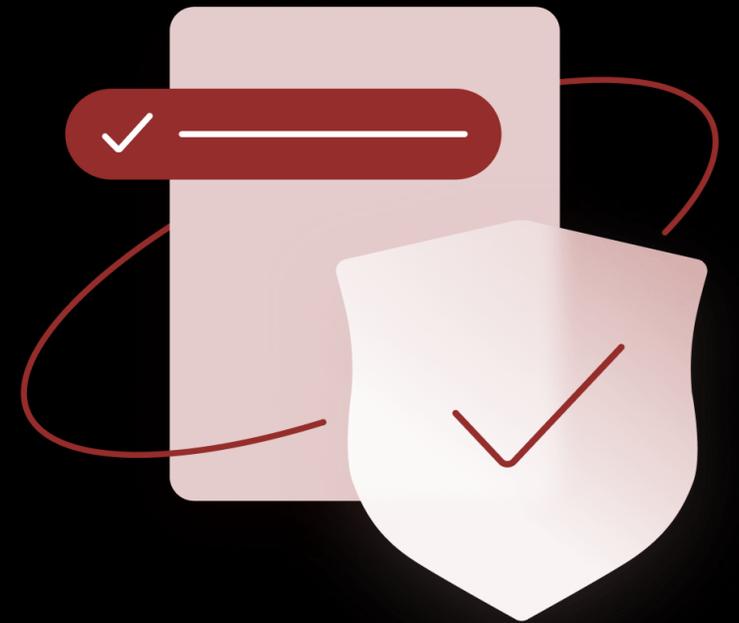


2FA как способ защиты УЗ сотрудников от несанкционированного входа

Дмитрий Мельников

Менеджер проектов по
внедрению Контур.ID

Контур



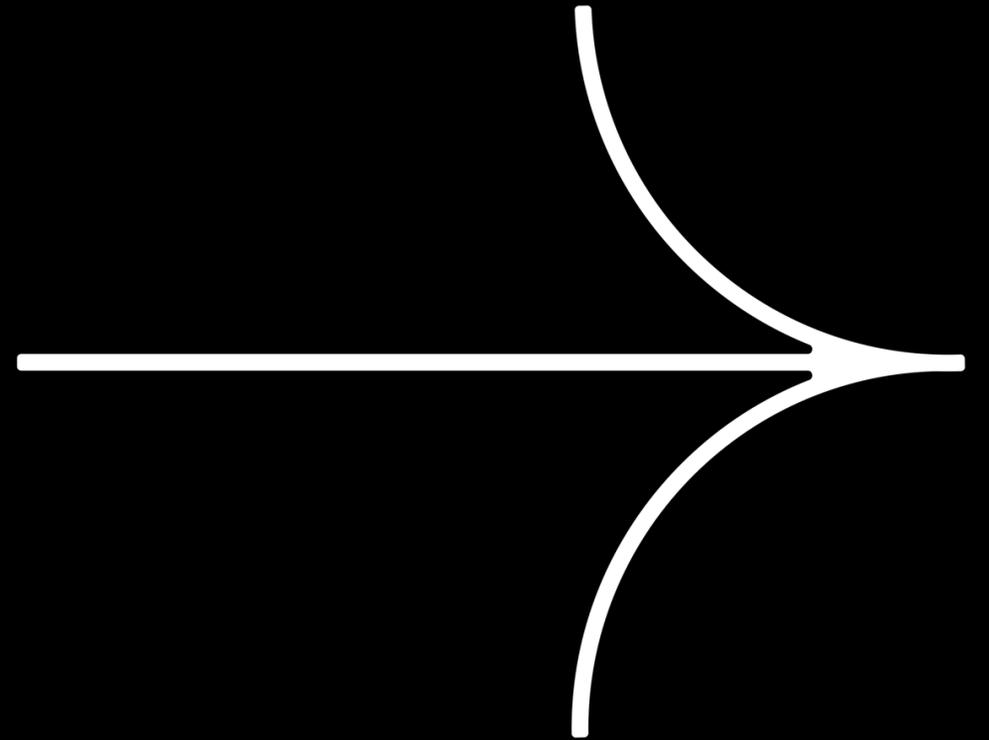
Дмитрий Мельников

Менеджер проектов по внедрению



Контур

**Проблематика
кибербезопасности –
с какими вызовами
сталкиваются
современные
компании**



ПРОБЛЕМАТИКА КИБЕРБЕЗОПАСНОСТИ

Векторы проникновения в сети компаний

63% ВЕБ-ПРИЛОЖЕНИЯ

наиболее часто почтовый сервер Microsoft Exchange (50% всех атак, веб-сервер Bitrix (13%) и продукты компании Atlassian (7%), например Confluence и Jira.

10% ДАННЫЕ СОТРУДНИКА

Утечки аутентификационных данных сотрудников

8% СЕРВИСЫ ИЗВНЕ

Доступные извне сервисы, не относящиеся к веб-сервисам

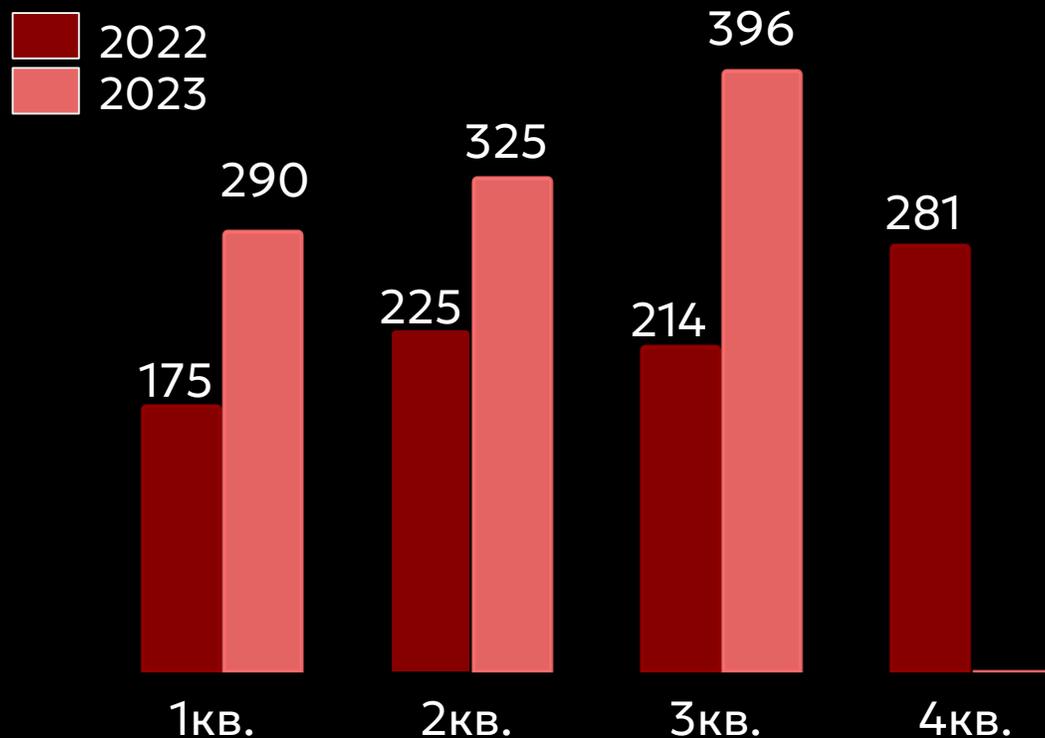
17% ФИШИНГОВЫЕ ПИСЬМА

Фишинговые письма направляемые на электронную почту.

2% УЯЗВИМОСТИ НУЛЕВОГО ДНЯ

СОБЫТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

Распределение событий ИБ по кварталам, тыс.



1 млн событий ИБ за 1-3 кв. 2023 года, что



на **64%** больше, чем в 1-3 кв. 2022г.

ПРОБЛЕМАТИКА КИБЕРБЕЗОПАСНОСТИ

Последствия атак

Влияние на бизнес -
процессы компании



32%

Разведка, шпионаж



32%

Выгрузка
конфиденциальной
информации



26%

Не удалось оценить

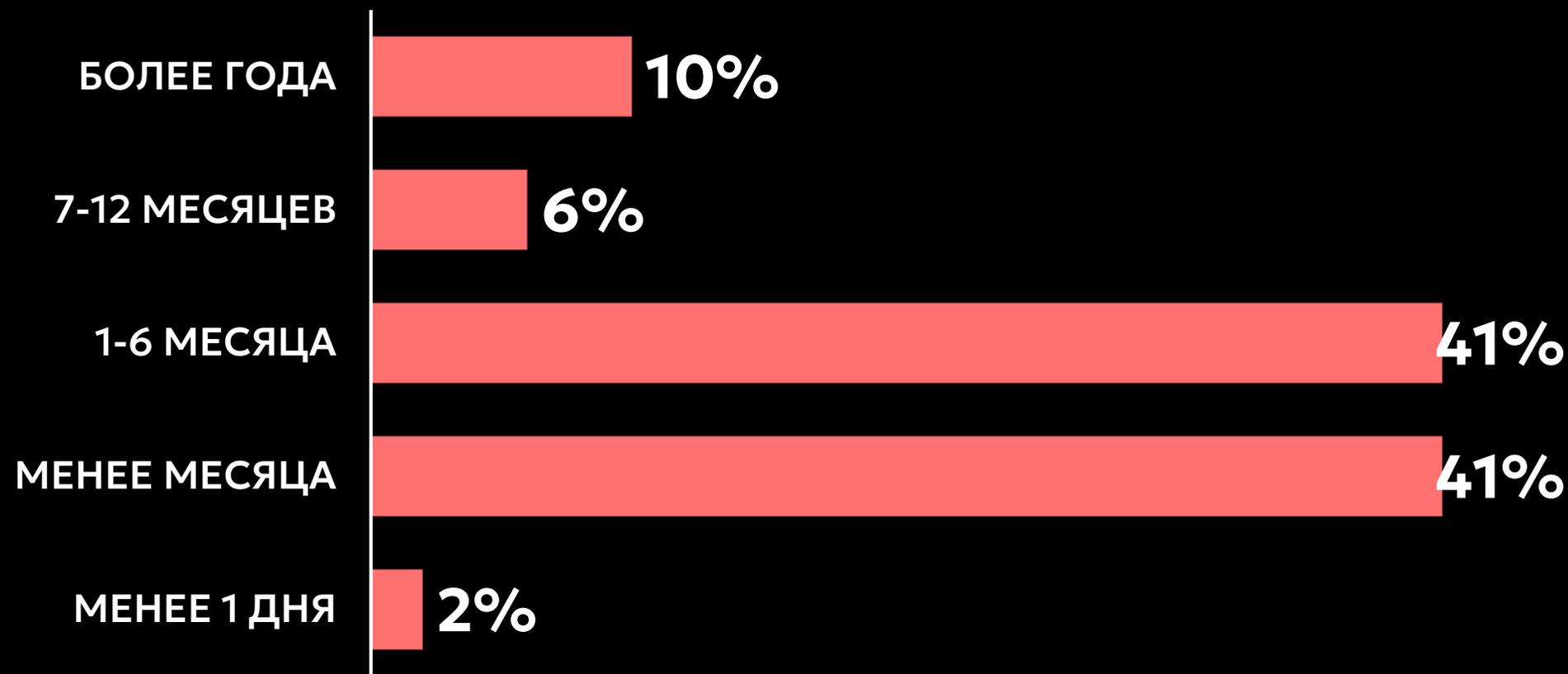


27%

4,45

млн долл. США
средний ущерб от
кибератак в 2023 году

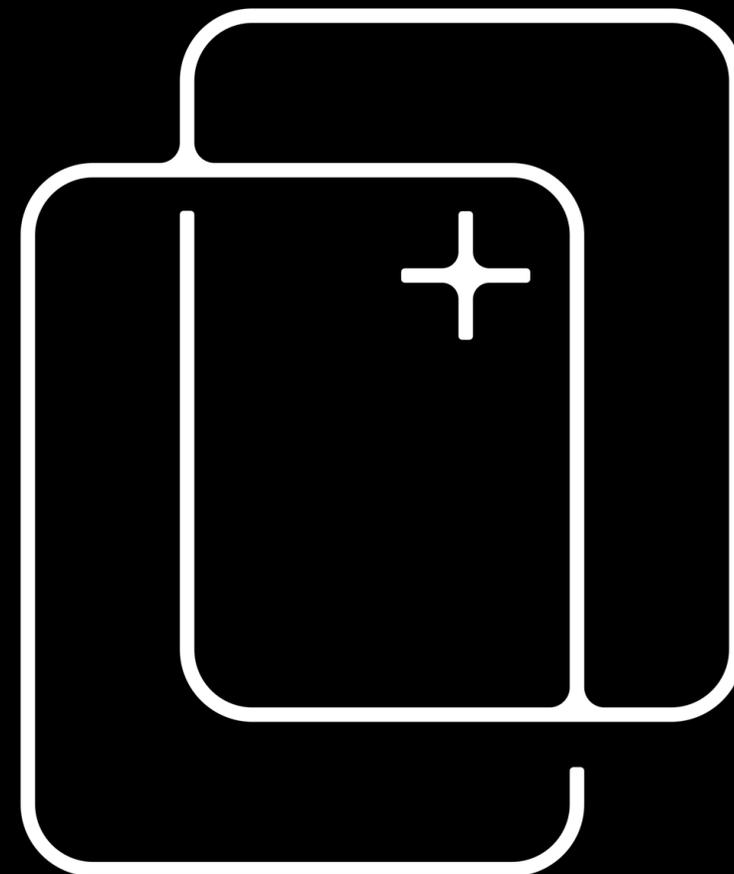
ВРЕМЯ ОБНАРУЖЕНИЯ КОМПРОМЕТАЦИИ



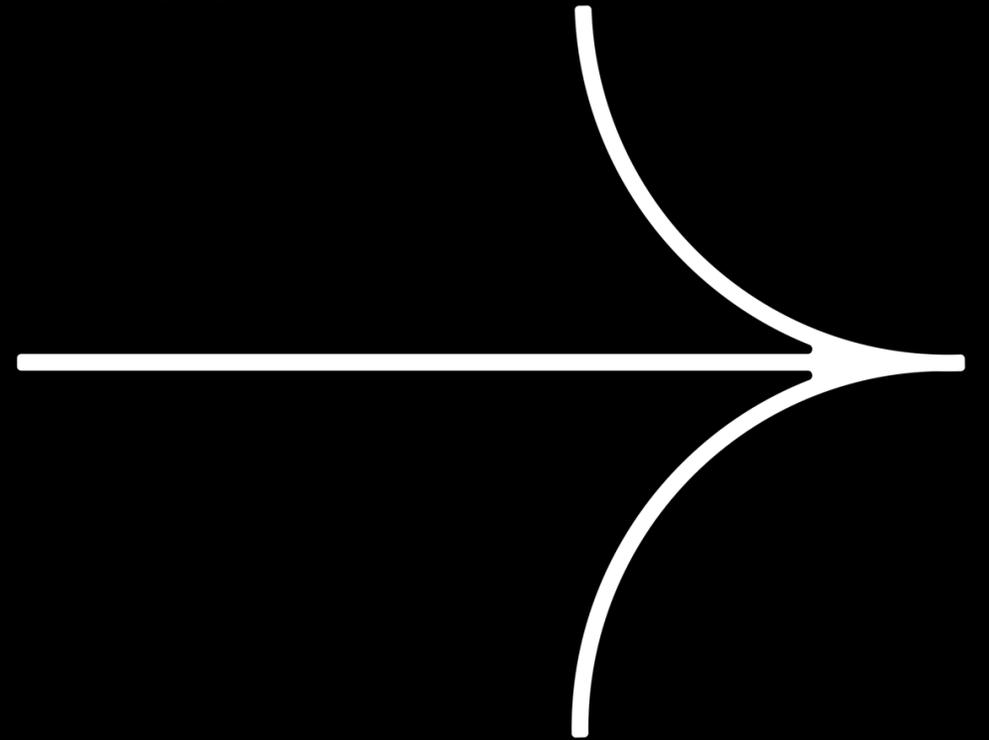
ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ

В Госдуму внесены поправки в КоАП, которые предусматривают многократное увеличение административных штрафов:

- от 3 до 5 млн рублей за утечку персональных данных от 1000 до 10 000 граждан;
- от 5 до 10 млн рублей при 10 000–100 000 пострадавших, а если их больше — то на сумму от 10 до 15 млн рублей.
- В случае повторного нарушения, независимо от объема дискредитированной информации, предлагается ввести штраф от 0,1 до 3% выручки за предшествующий календарный год, но не менее 15 млн и не более 500 млн рублей.



Способы защиты учетных записей сотрудников от несанкционированного входа



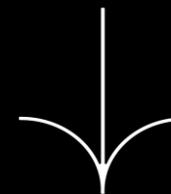
Способы защиты учетных записей сотрудников от несанкционированного входа

Аппаратные средства защиты

Программные средства защиты

Криптографическая защита

Программно-аппаратные средства защиты



Внедрение двухфакторной аутентификации

Один из лучших способов предотвратить несанкционированный доступ – это дополнить методы аутентификации.

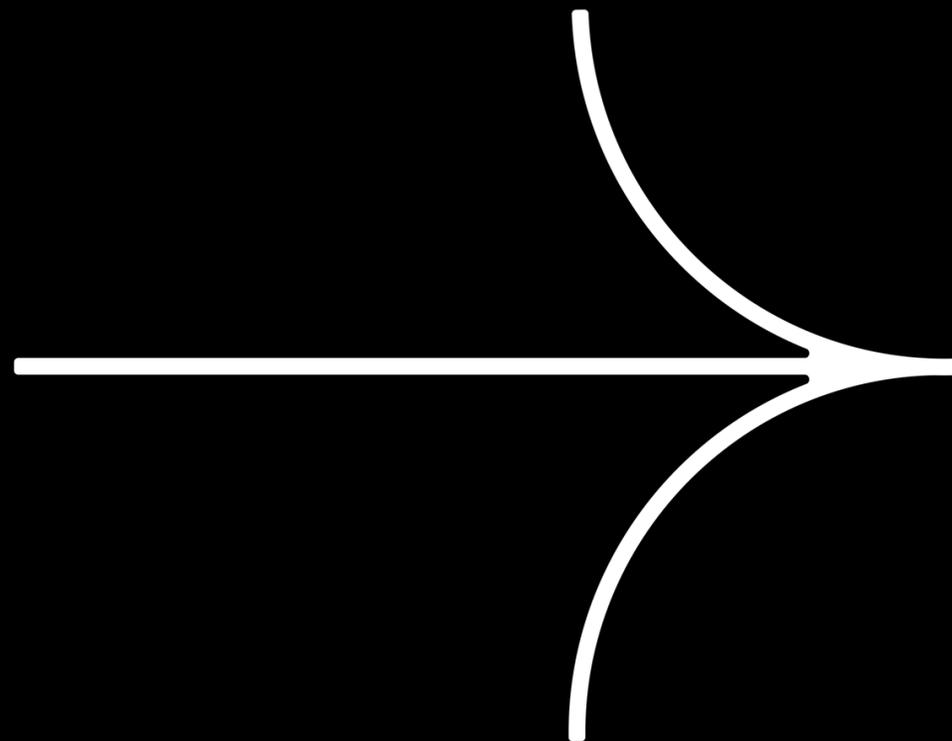
Использование нескольких факторов для доступа пользователей к чувствительным данным снижает:

- на **99,9%** вероятность успеха автоматизированной атаки на пользователя;
- на **96%** вероятность успеха при массовой фишинговой атаке;
- останавливает до **75%** всех целенаправленных атак.



Продукт Контур.ID – двухфакторная аутентификация

Защитит рабочие
аккаунты сотрудников
от взлома



Контур.ID

Проверенный производитель

Контур создает программное обеспечение для бизнеса с 1988 года

SLO – 99,99%

Доступность наших серверов – 99,99%

Широкая функциональность

Различные сценарии использования и способы аутентификации

Поддержка разработчиков

Помощь инженеров-экспертов внедрения и сопровождение в масштабировании

Собственные сервера

Дата-центры располагаются на территории РФ

Простота использования

Панель управления администратора, приложение Контур.Коннект – удобные и понятные решения

Возможности Контур.ID – двухфакторной аутентификации

Сейчас

- NPS
- VPN\WIFI (RADIUS)
- RDG
- OWA (IIS)
- ADFS
- ActiveSync

Скоро

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

Панель управления Контур.ID

Контур ID

- Ресурсы
- Пользователи

Документация

ООО "Звёздочка"

Пользователь

Ресурсы



Open VPN
261 конфигурация

Создать конфигурацию



Cisco Any Connect
98 конфигураций

Создать конфигурацию



Checkpoint
26 конфигураций

Создать конфигурацию



RDP
91 конфигурация

Создать конфигурацию



AD FS

Настроить



Outlook Web

Настроить



ActiveSync
12 конфигураций

Создать конфигурацию

СКБ Контур с 1998 года

Как работает двухфакторная аутентификация ?

Личный кабинет и приложение

Контур ID OOO Интеркомрамо 

Настройте Контур.Коннект

Приложение позволит подтверждать подключения к корпоративным ресурсам

[Начать настройку](#)



Доступ к почте и календарю

Почтовые клиенты, у которых есть доступ к вашей корпоративной почте и календарю

Запрашивают доступ

 Android Android 16.0.3 20A392, подключено 20.02.2023, 14:28	Отклонить	Разрешить
 WindowsMail Windows 16.0.3 20A392, подключено 20.02.2023, 14:28	Отклонить	Разрешить

Синхронизируются

 Android Android 16.0.3 20A392, подключено 20.02.2023, 14:28	
 Android Android 16.0.3 20A392, подключено 20.02.2023, 14:28	



Кто-то пытается войти в ваш аккаунт

Подтвердите или заблокируйте вход в [название площадки] под [почта регистрации]

[Всё хорошо, это я](#)

[Заблокировать вход](#)

On-cloud

1 ПРОСТОТА РАЗВЕРТЫВАНИЯ

Экономия человеческих ресурсов на установку и поддержку.

2 ДОСТУПНОСТЬ

Нет необходимости приобретать и обслуживать дополнительные сервера.

3 БЕЗОПАСНОСТЬ

Аттестованные сервера
Находятся в России

4 УДОБСТВО

Сопровождение отделом внедрения и наличие технической поддержки

On-premise

Реализация «коробки»

в планах на конец 2024 года

DMZ

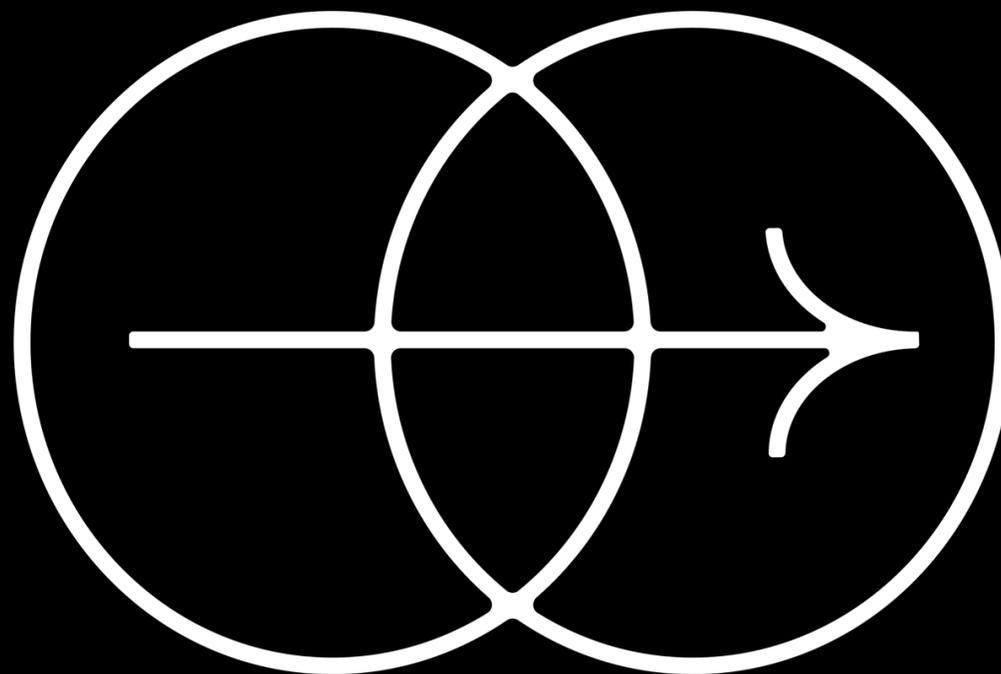
как альтернатива

Регистрируйтесь на бесплатное тестирование

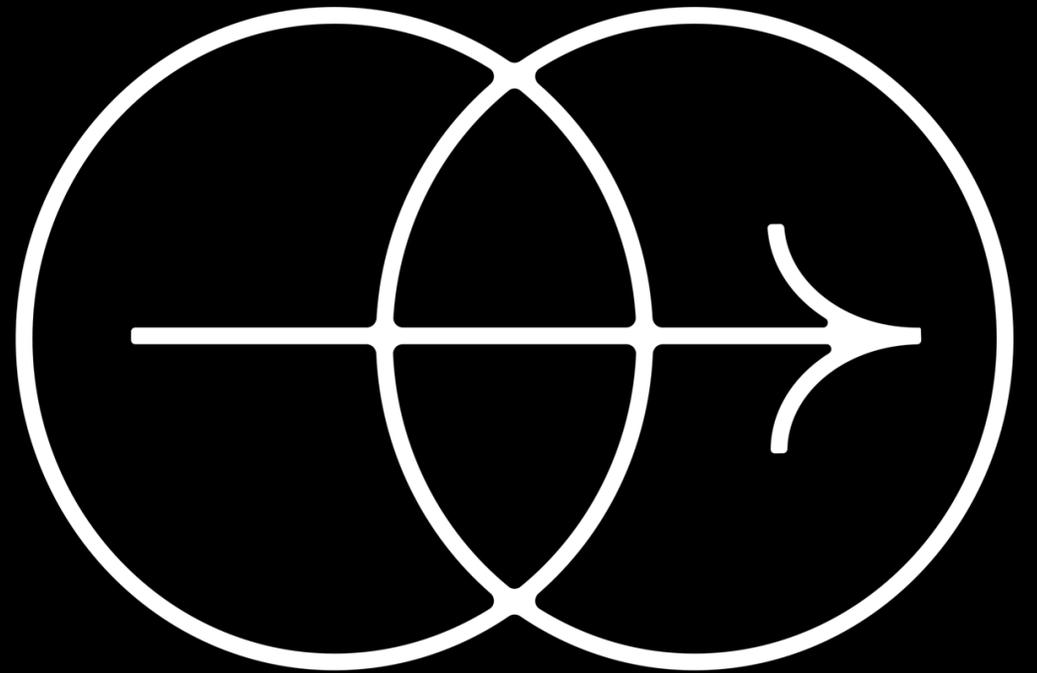


Дмитрий Мельников

Вопросы



Back up



Почему облако удобнее чем он-прем?

Параметр	On-prem	On-cloud
Скорость разворачивания	Долго От нескольких недель	Быстро От нескольких часов
Масштабируемость	Дорого и долго Закупка нового оборудования Настройка новых серверов	Быстро и не дорого В пару кликов расширяется количество лицензий и новые пользователи уже могут войти
Затраты	Большие Оборудование и его обслуживание Персонал и его обучение Возможные изменения в архитектуре компании	Не большие Оплата за количество пользователей Остальные затраты берет на себя сервис

Схема 2ФА в VPN/RDP

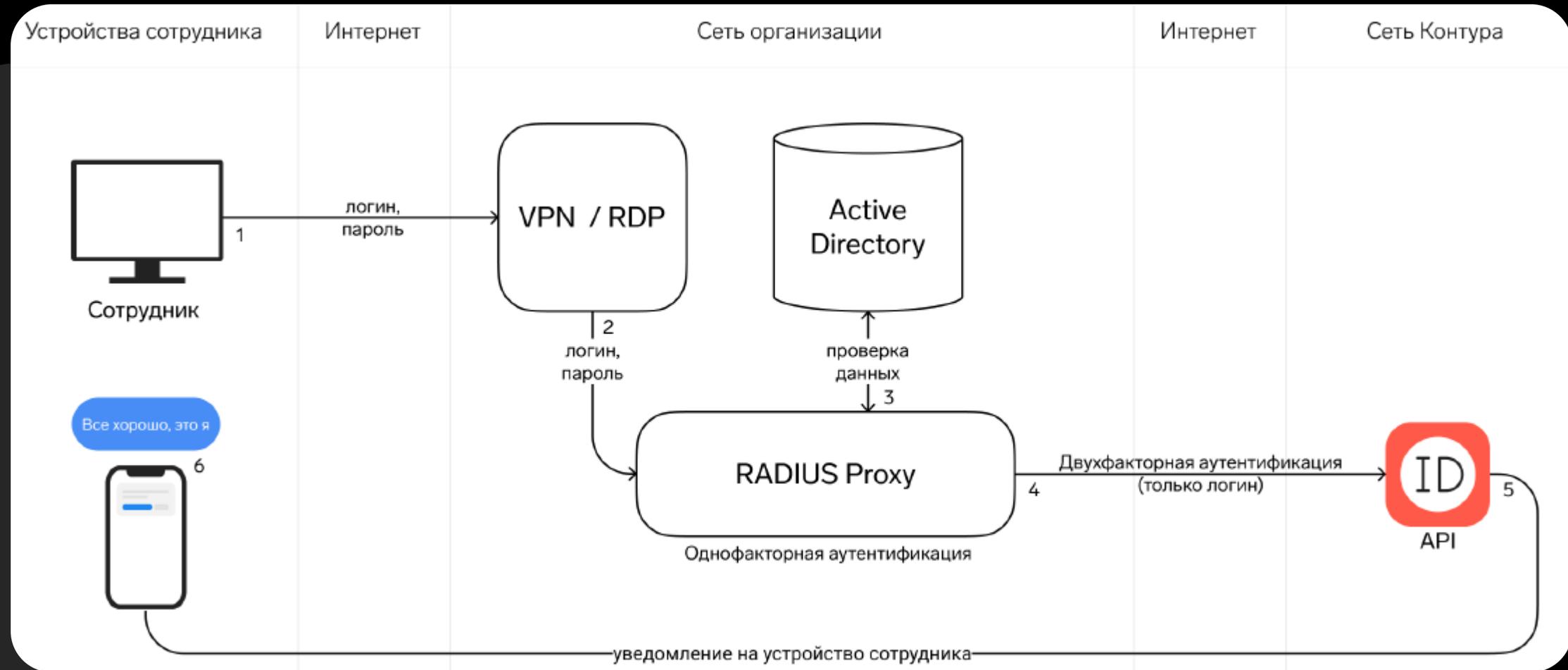
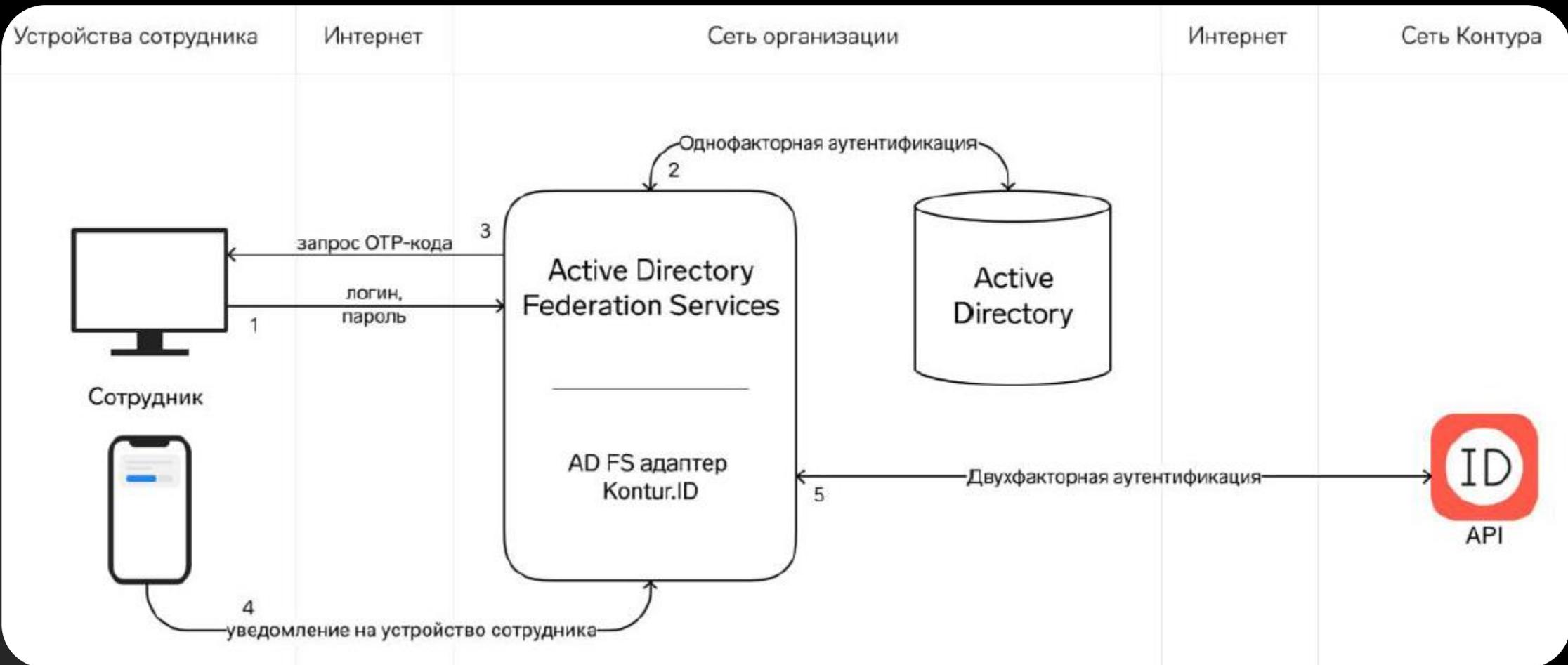


Схема 2ФА в ADFS



Exchange. ActiveSync

