

Будущее удаленной работы: безопасный доступ в эпоху облаков и AI



Сергей Михайлюк, CISO

Удаленный доступ как норма

- Более 70% компаний перешли на гибридный режим.
- Это удобно для сотрудников и бизнеса.
- Но небезопасные подключения = риск для компании.



Как раньше интернет был только в офисе, а теперь — в телефоне у каждого. Работа стала такой же мобильной.

VPN и старый периметр

- Раньше: «офис + VPN» = основная защита.
- Минусы: неудобно, уязвимо, трудно масштабировать.
- Через слабый VPN можно попасть в сеть компании.



VPN — это как тайный туннель в офис. Но если враг узнает вход — он тоже попадёт внутрь.

Периметра больше нет

- Люди работают в облаках: документы, чаты, CRM.
- Каждый сотрудник = отдельная точка доступа.
- Ошибка одного может ударить по всей компании.



Раньше компания была как крепость. Сейчас это сеть калиток — достаточно открыть одну, чтобы попасть внутрь.

Zero Trust ВМЕСТО ДОВЕРИЯ

- Проверяется каждый запрос и каждое устройство.
- Доступ — только к нужным данным.
- Риск утечек снижается.



Как на концерт: проверяют и билет, и паспорт, даже у артистов. Так и в Zero Trust.

Без паролей: новая аутентификация

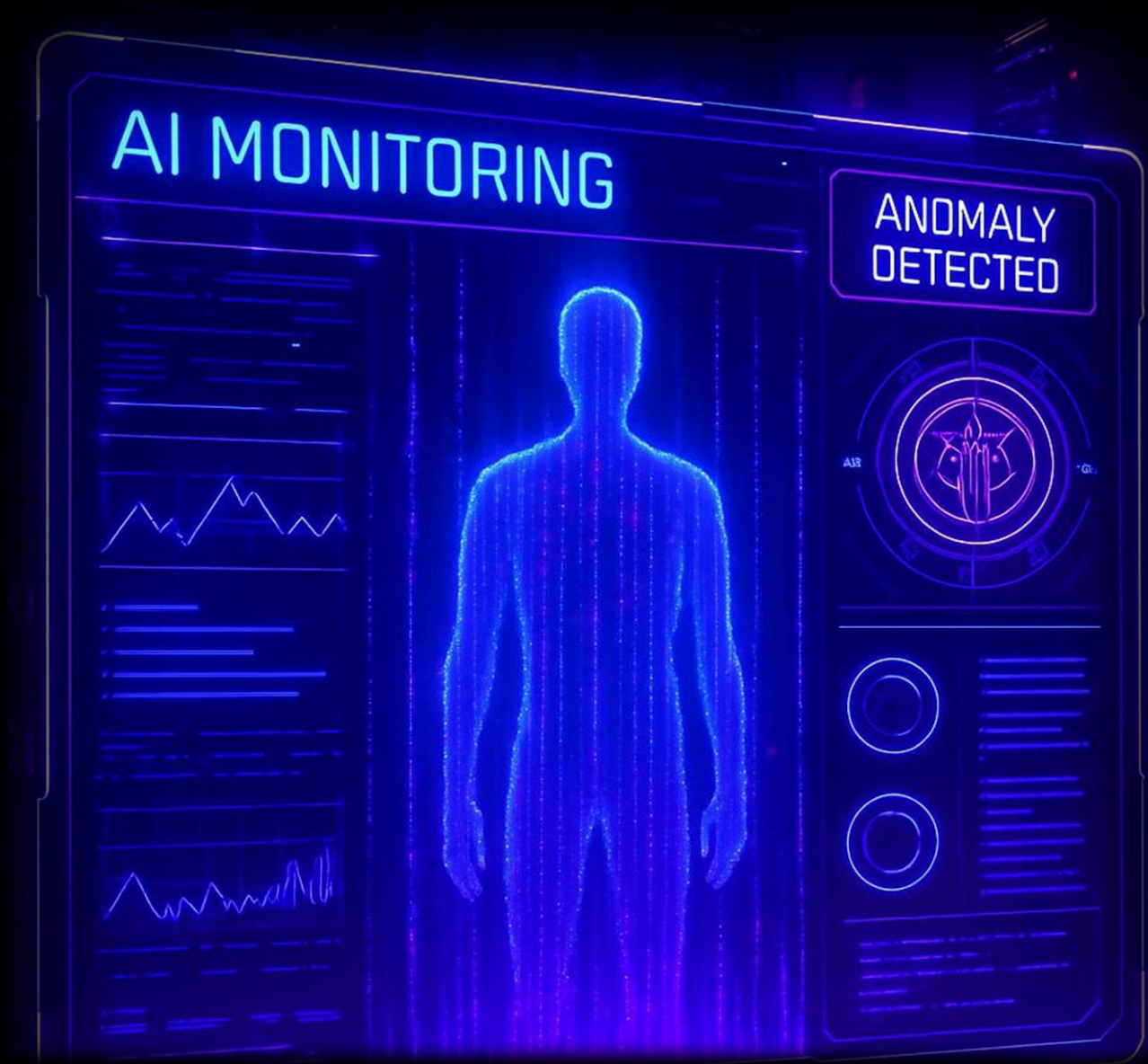
- Пароли устарели: их крадут или подбирают.
- Будущее — биометрия, коды, ключи-брелоки.
- Это и удобнее, и безопаснее.



Пароль = обычный ключ. Его можно потерять или украсть. Биометрия = замок, который открывается только вашим пальцем.

AI как новый рубеж

- AI следит за подключениями.
- Замечает подозрительное поведение.
- Может автоматически заблокировать угрозу.



Как охранник, который никогда не спит: если кто-то заходит в дом ночью через окно — он мгновенно поднимает тревогу.

Сложности и барьеры

- Новые технологии стоят дорого.
- Нужно учитывать законы и требования.
- Люди часто сами нарушают правила.



Сотрудники пишут пароли на стикерах — и самая сильная защита становится бесполезной.

Реалии и импортозамещение

- Нужно использовать отечественные решения.
- Они пока слабее западных, но рынок растёт.
- Уже сегодня можно выстроить защищённый доступ.



Это как российские смартфоны — пока не такие удобные, но соответствуют закону и позволяют работать.

Что делать компаниям?

- Проверять каждого (Zero Trust).
- Уйти от паролей → биометрия, MFA.
- Подключить AI для обнаружения угроз.
- Обучать сотрудников простым правилам.



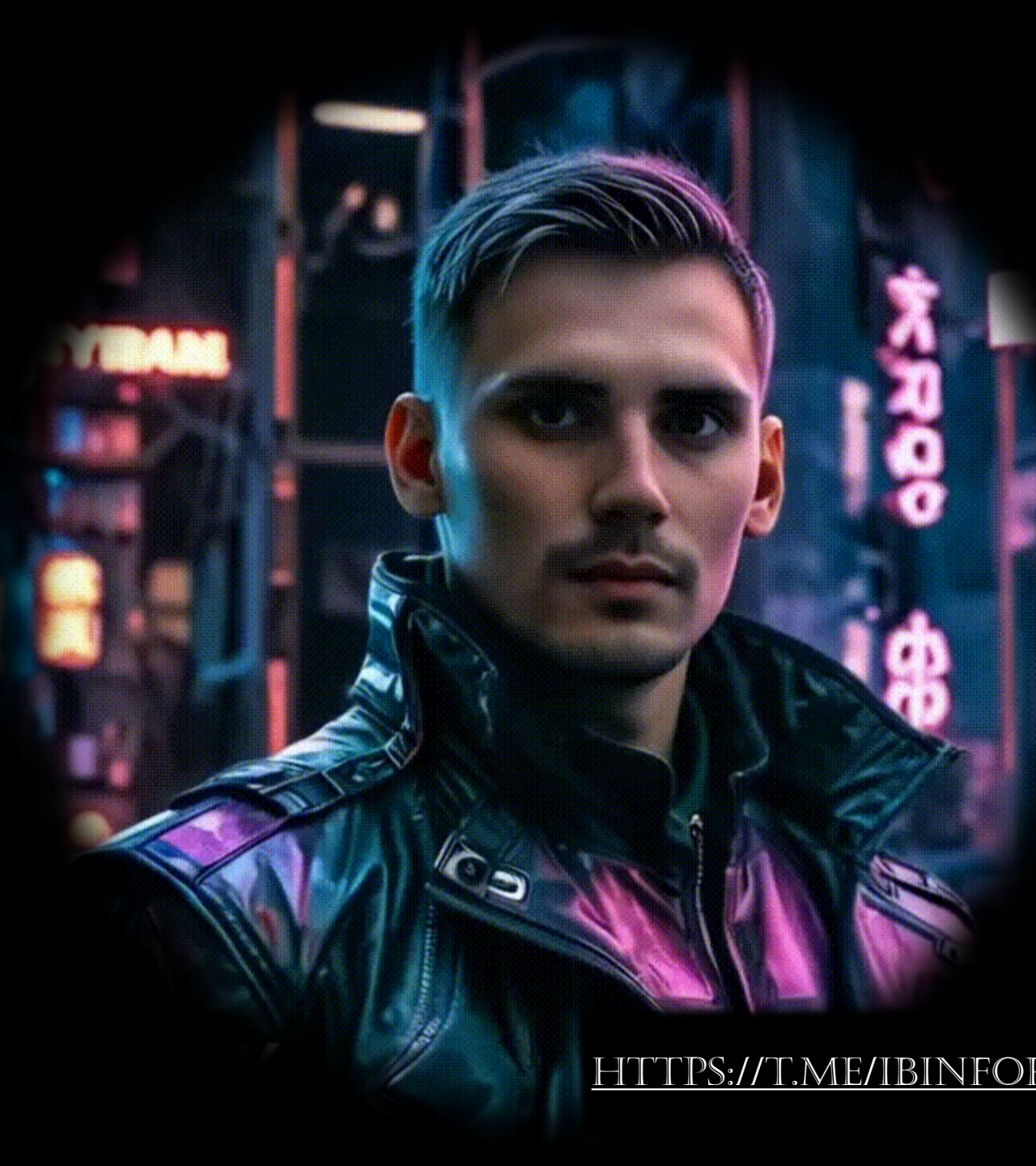
Как ремонт: сначала двери и окна (MFA), потом сигнализация (Zero Trust), потом камеры (AI).

Будущее безопасного доступа

- Работа из любой точки мира = стандарт.
- Безопасный доступ повышает продуктивность.
- Это становится преимуществом бизнеса.

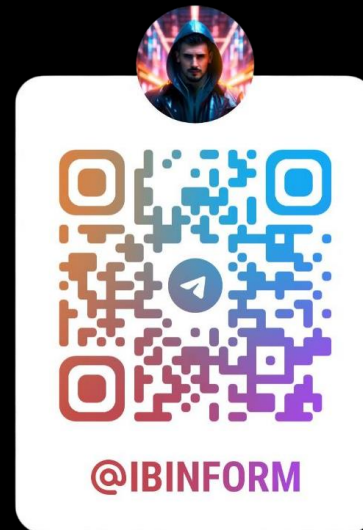


Как Wi-Fi: должен работать везде, но доступ только у тех, у кого есть ключ.



itsec® ИНФОРМАЦИОННАЯ
И КИБЕРБЕЗОПАСНОСТЬ
РОССИИ

Спасибо !



[HTTPS://T.ME/IBINFORM](https://t.me/IBINFORM)