Особенности работы распределённых команд в ИБ: опыт заказчика

Константин Саматов

Член правления АРСИБ (Ассоциация руководителей служб ИБ)

Распределённая работа — новая норма

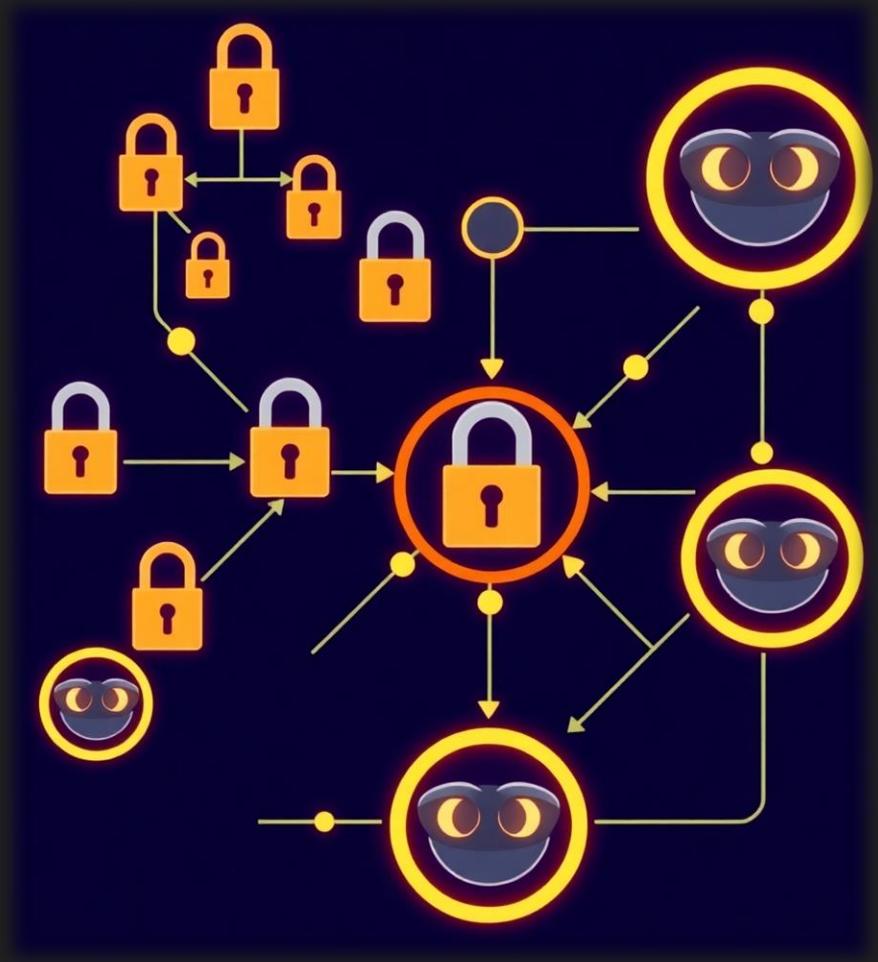
- Крупная филиальная сеть
- Удалённые сотрудники
- Региональные команды
- Подрядчики

Ключевые вызовы

- Утечка данных и потеря контроля
- Недоверие к внешним участникам
- Отсутствие единой политики доступа
- Риски при работе с КИИ и персональными данными
- Сложности в контроле и мониторинге

Что нужно для безопасной удалёнки

- Многофакторная аутентификация
- Минимизация привилегий
- Защищённые каналы
- Полный аудит и логирование
- Контроль среды устройства



Организационные меры

- Регламентация удалённого доступа
- Формализация ролей и полномочий
- Соглашения по SLA и ответственности
- Инструктажи и обучение
- Централизованный контроль и координация

Технические подходы

- PAM-системы для управления привилегиями
- Виртуальные рабочие столы и терминальные решения
- Контроль доступа по сессиям и времени
- Интеграция с SIEM и IDM

Практические сценарии: удаленные работники

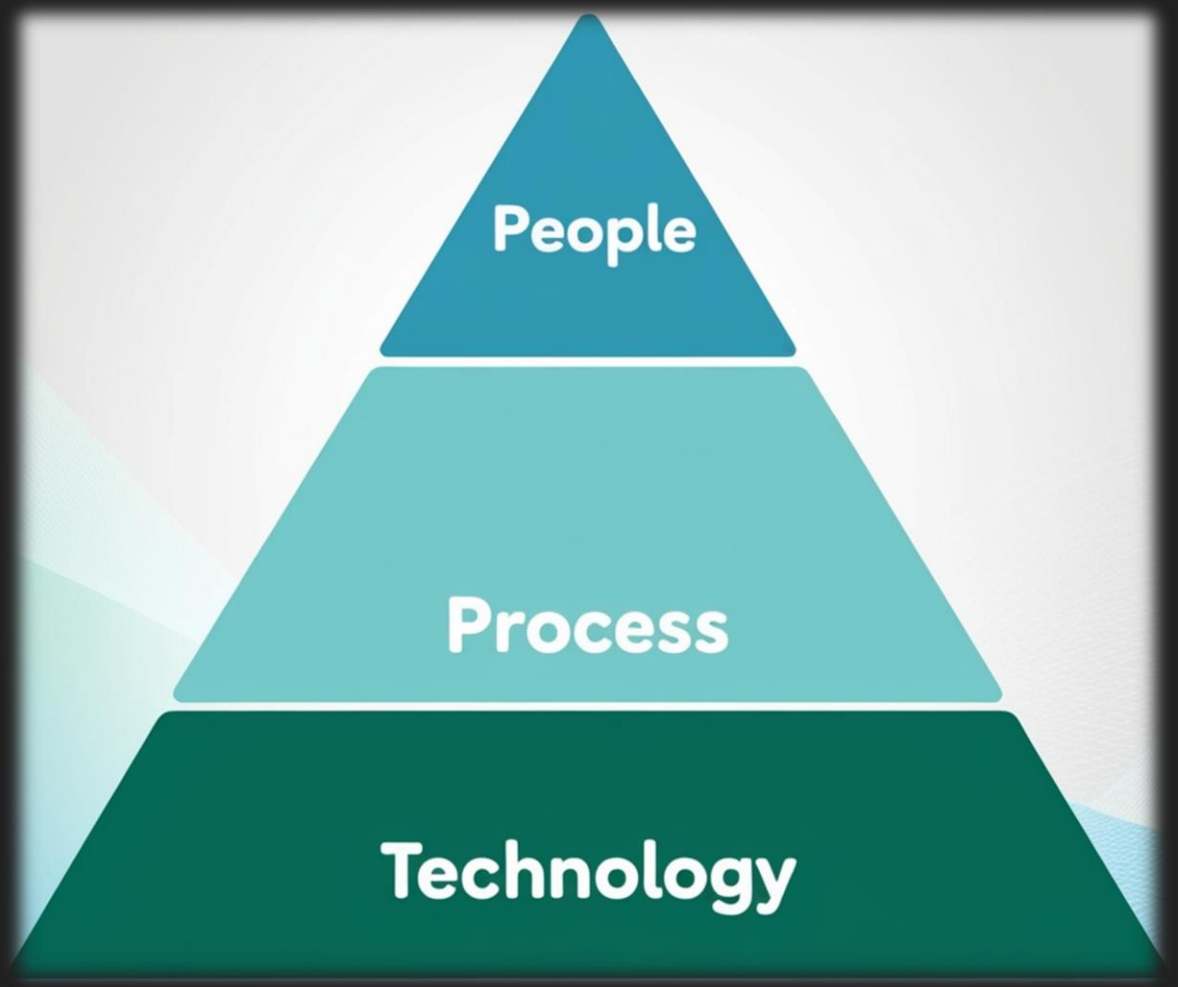
- Доступ из домашней сети → повышенные риски
- Использование личных устройств (BYOD) — сложность контроля
- Необходимость защищённого канала (VPN)
- Обязательная настройка политики на устройствах (антивирус, шифрование, блокировка внешних носителей)
- Логирование и мониторинг всех действий

Практические сценарии: подрядчики

- Временный или эпизодический доступ к ИТ-инфраструктуре
- Необходима обязательная авторизация, регистрация и аудит
- Чёткое разграничение зон доступа и задач
- Проверка подрядчика: ИБ-профиль, соглашения по SLA, ответственность

Рекомендации

- Начинайте с процессов, не с технологий
- Контролируйте не только «кто», но и «как»
- Обучайте — это не затраты, а инвестиции



Спасибо за внимание!

Защищённый удалённый доступ — это комбинация зрелых процессов, технических решений и управляемой культуры безопасности