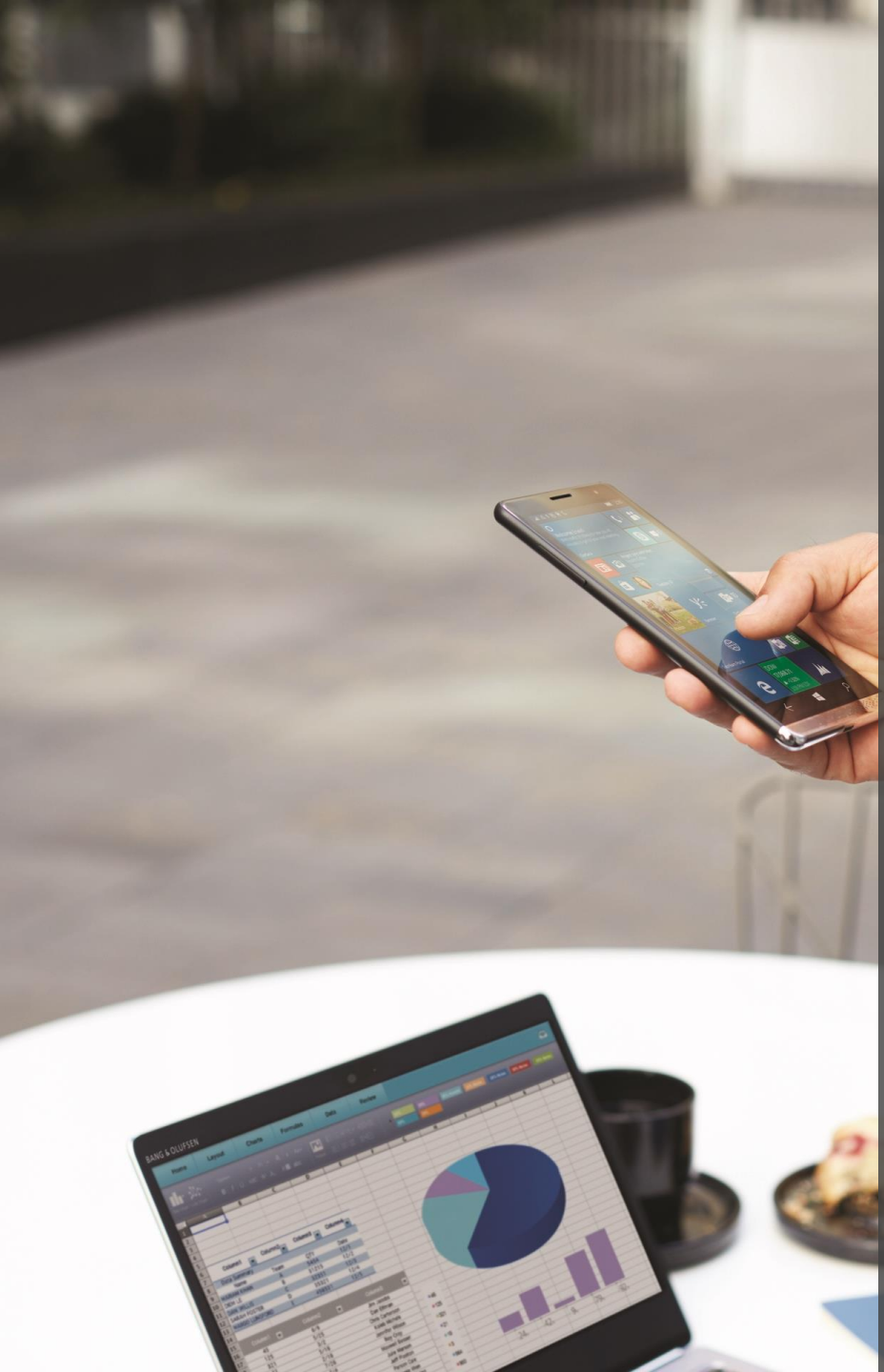


INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

МОБИЛЬНЫЕ УСТРОЙСТВА & DLP – ВОЗМОЖЕН ЛИ АЛЬЯНС?

Александр Клевцов
менеджер по развитию продуктов
InfoWatch

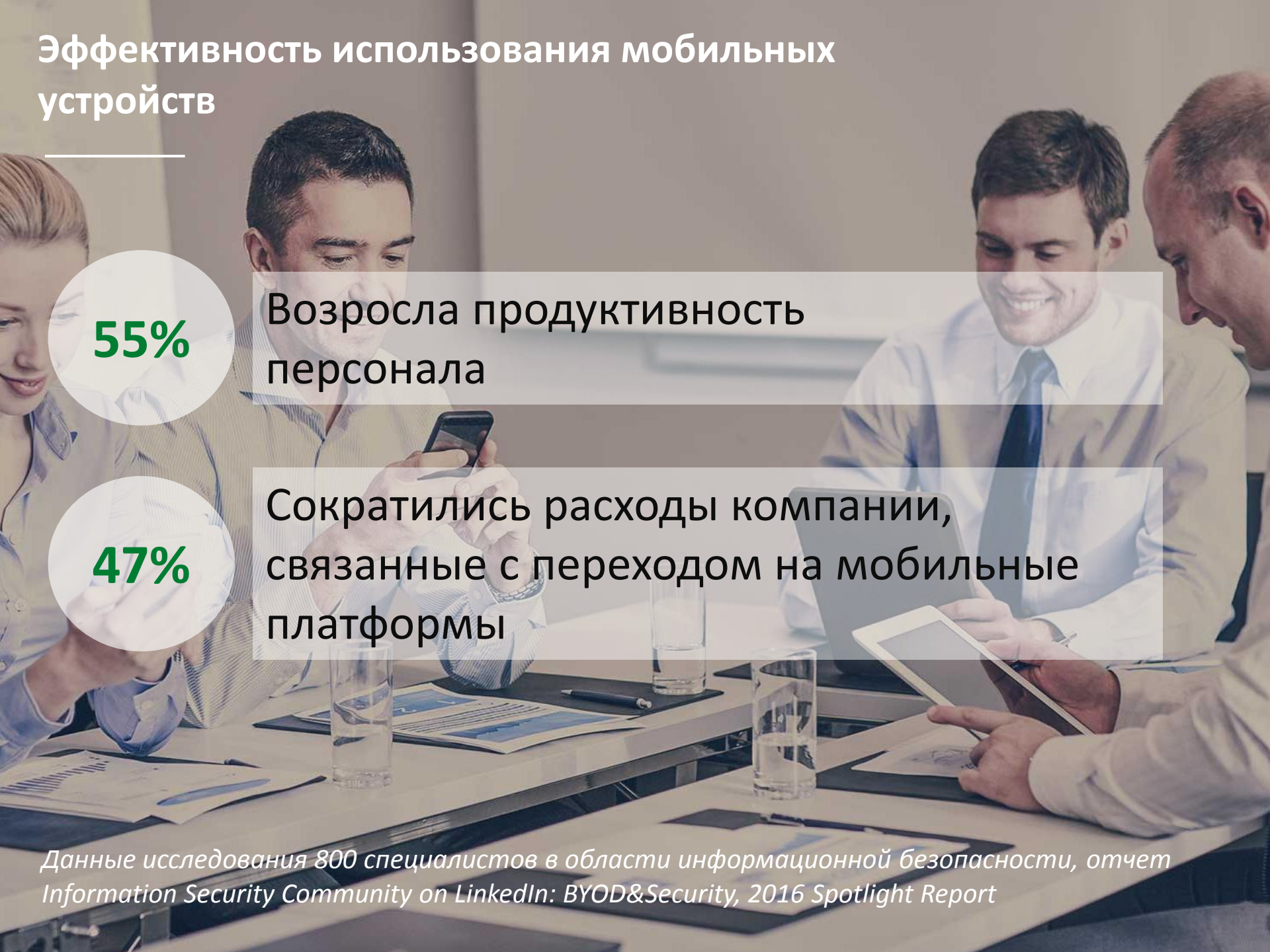
Использование мобильных устройств в корпоративной среде: текущая ситуация

> 75% российских компаний разрешают сотрудникам использовать мобильные устройства для работы

> 50% российских компаний разрешен доступ к корпоративной почте с мобильного устройства

** Данные исследования корпоративной мобильности в России. Источник MobilityLab:*
http://www.workspad.ru/resources/analitika/workspad-byod-survey/

Эффективность использования мобильных устройств



55% Возросла продуктивность персонала

47% Сократились расходы компании, связанные с переходом на мобильные платформы

Данные исследования 800 специалистов в области информационной безопасности, отчет Information Security Community on LinkedIn: BYOD&Security, 2016 Spotlight Report

Что насчет безопасности?

«Вы же сказали, я могу приносить свои личные устройства!»

15% Несоблюдение сотрудниками политик безопасности

19% Утечки данных с мобильных устройств

** Исследование MobilityLab, 2011-2016*

Кейс. Утечки данных через мобильные устройства

INFOWATCH®

PNC BANK

Злоумышленник	Сценарий	Ущерб
Топ-менеджер PNC Bank Эйлин Дейли	**Фотографировала экран** своего компьютера со стратегической информацией на смартфон незадолго до увольнения	По оценкам PNC Bank, ущерб от действий бывшего топ-менеджера составил **250 млн. $**

INFOWATCH®

Как обеспечить безопасность

при этом

сохранить мобильность сотрудников?

Экосистема устройств, используемых в корпоративной среде

INFOWATCH®

Риски

Личные устройства сотрудников

Корпоративные мобильные устройства

Стационарные корпоративные устройства

«Свобода» устройства

Корпоративные мобильные устройства

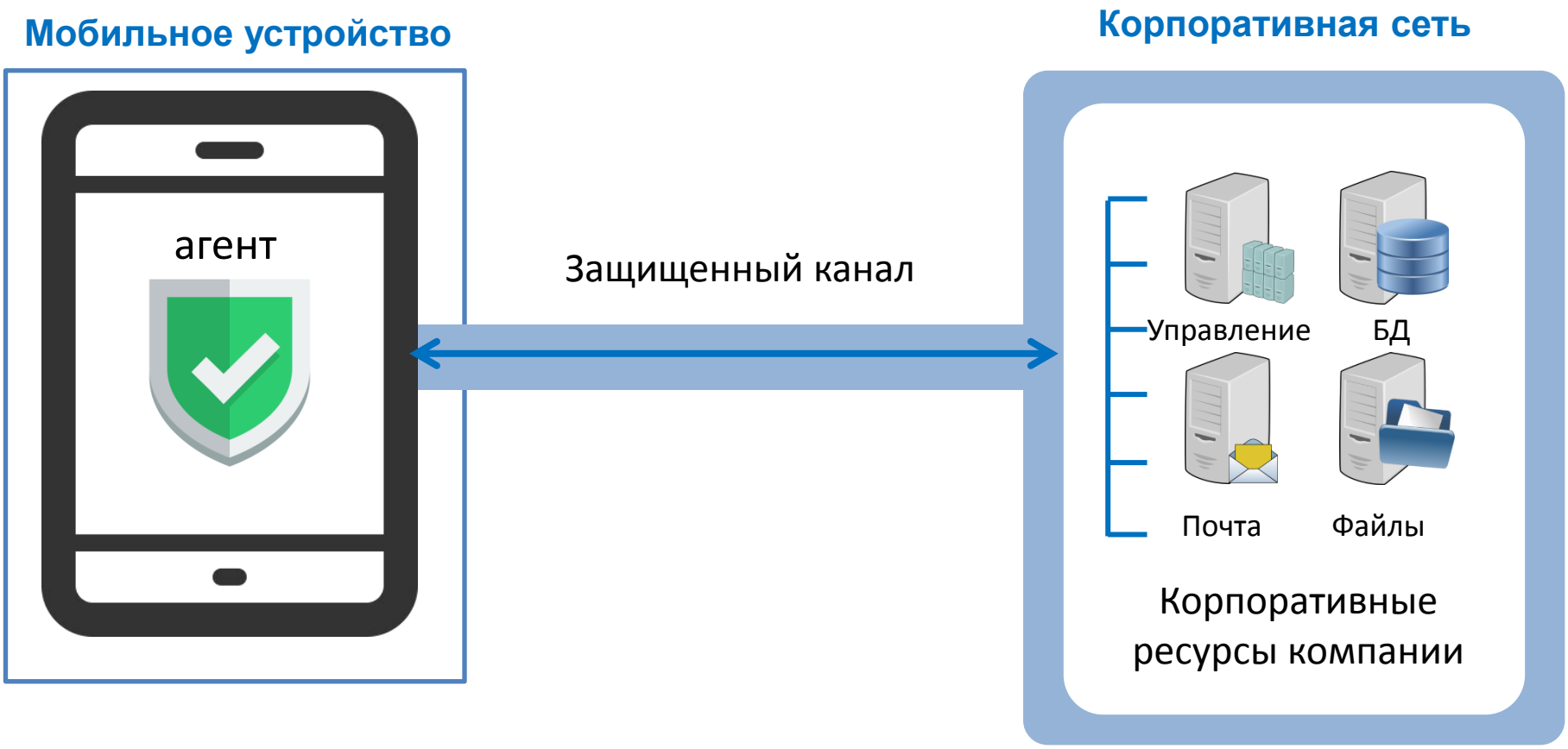
- Корпоративные ноутбуки
- Корпоративные смартфоны, планшеты

Все под контролем:

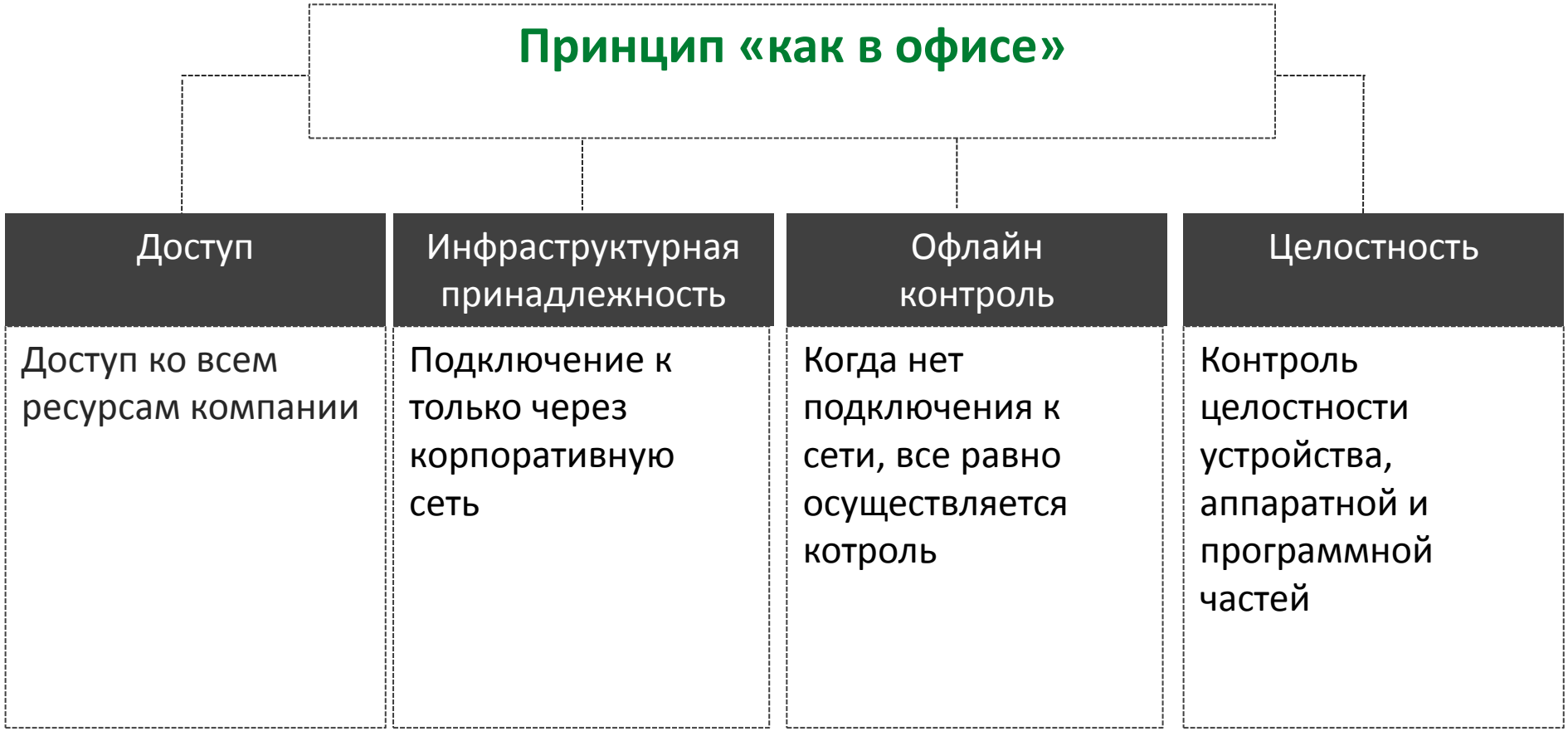
✓ Устройство привязано к сотруднику

✓ Компания определяет аппаратные и программные компоненты устройства

Агентское решение: принцип «как в офисе»



Принцип «как в офисе»



Корпоративные мобильные устройства: требования к средствам защиты

- Контроль сетевых соединений
- Запрет использования устройств/компонентов
- Контроль каналов передачи данных (блокировка по результатам анализа)
- Контроль загрузки и целостности агента
- Контроль использования приложений
- Инвентаризация аппаратной и программной частей
- Шифрование данных и съемных носителей

Рецепт безопасности личных рабочих станций

Агентский модуль InfoWatch Traffic Monitor

+

VPN

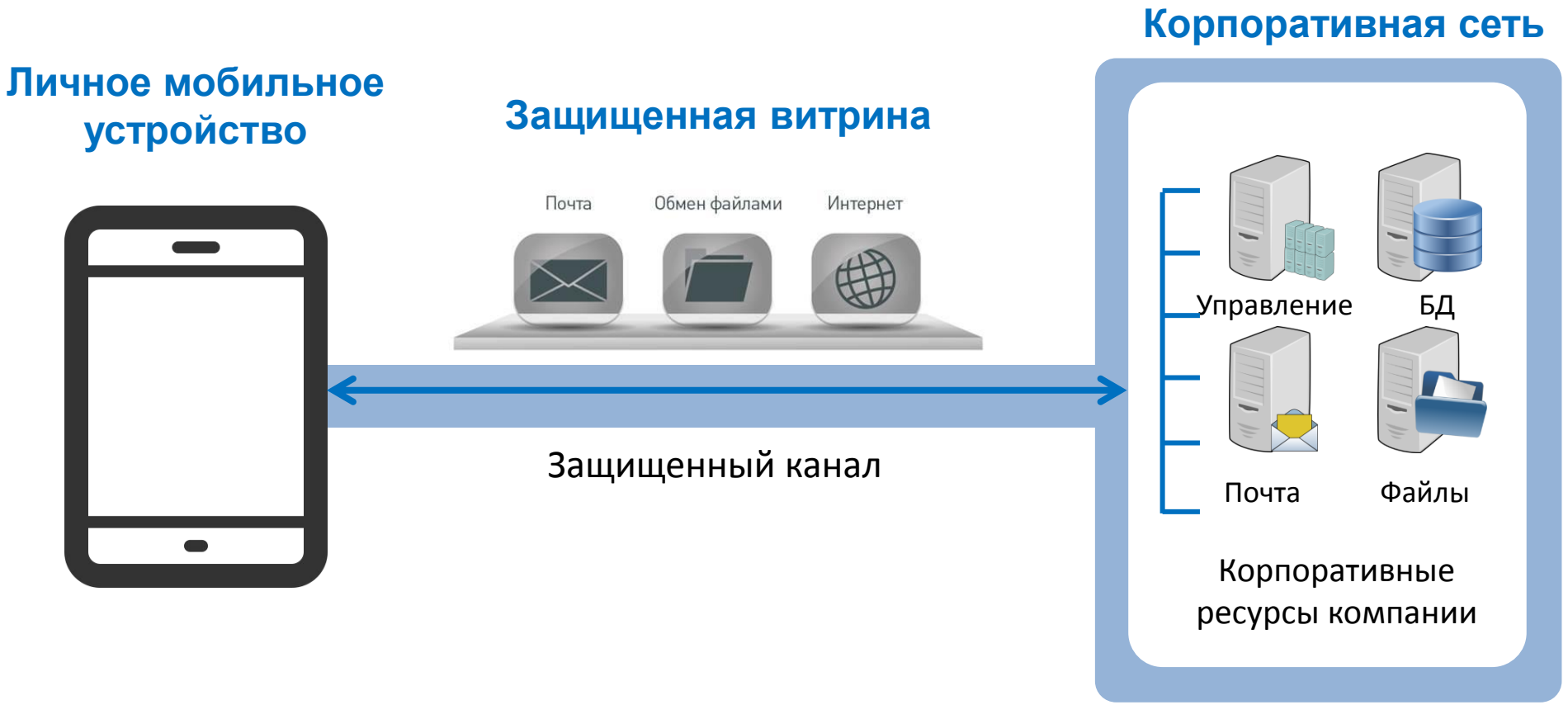
Личные устройства сотрудников

- Домашние рабочие станции удаленных сотрудников
- Личные мобильные устройства сотрудников

✓ У каждого сотрудника может быть **несколько устройств**
✓ Личные мобильные устройства в любой момент могут быть **обнулены, заменены, обновлены** и т.д.
✓ Сотрудники **отказываются устанавливать средства контроля** на личные мобильные устройства

Защищенная витрина

INFOWATCH®



Личные мобильные устройства: концепция безопасности

INFOWATCH®

Концепция защищенной витрины

Мотивация	Монополия	Контейнер	Независимость
• Выполнение производственных обязанностей • Удобство использования	• Единая точка доступа для всех корпоративных ресурсов • Потребность в owa автоматически снимается	• Недоступность данных на устройстве • Невозможность их сохранения во внутренней памяти устройства	• Неважно, какой моделью устройства / операционной системой пользуется сотрудник

Личные мобильные устройства - инфраструктура

- VPN
- Решение, обеспечивающее точку доступа на мобильном устройстве (Airwatch, Workspad, MobileIron, Citrix XenApp)
- Интеграция серверной части точки доступа с решение DLP

VPN + EMM (VDI) + DLP

Рецепт безопасности личных мобильных устройств

Безопасное мобильное рабочее место: единое решение для обеспечения мобильного доступа сотрудников к рабочей среде

INFOWATCH®

WorksPad

INFOWATCH®

infotecs®

Безопасная среда

- **контейнер** приложения
- **управляемый доступ** к корп. ресурсам
- политики безопасности: **open-in, copy-past, wipe/lock**

Контролируемая безопасность

- создание **контролируемого периметра**
- **контроль информационных потоков** на мобильном устройстве
- **контроль** удаленных **сотрудников**
- проведение **расследований**

Шифрование данных

- **защищенный канал** доступа к корпоративным ресурсам
- **шифрование данных** в контейнере
- сертификация **ФСБ**

INFOWATCH®

Корпоративные устройства – Агентское решение

Личные устройства – Защищенная витрина

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

СПАСИБО ЗА ВНИМАНИЕ!
ДАВАЙТЕ ОБСУДИМ?

Александр Клевцов
менеджер по развитию продуктов, InfoWatch

Alexander.Klevtsov@infowatch.com