ЭЛВИС-ПЛЮС

Устройства, люди и документы - управляемый «хаос»
Mobile Device Management, MDM

InfoSecurity Russia'2014| Крокус Экспо|24.09.2014

О чем пойдет речь

1. Целесообразность использования мобильных устройств в компании.
2. Возможные проблемы, связанные с мобильными устройствами.
3. Подходы и инструменты для безопасного использования мобильных устройств.
4. Сценарий реализации MDM.
5. Некоторые выводы про безопасность и мобильные устройства.

Компания ОАО «ЭЛВИС-ПЛЮС»

1991 год – основание компании.

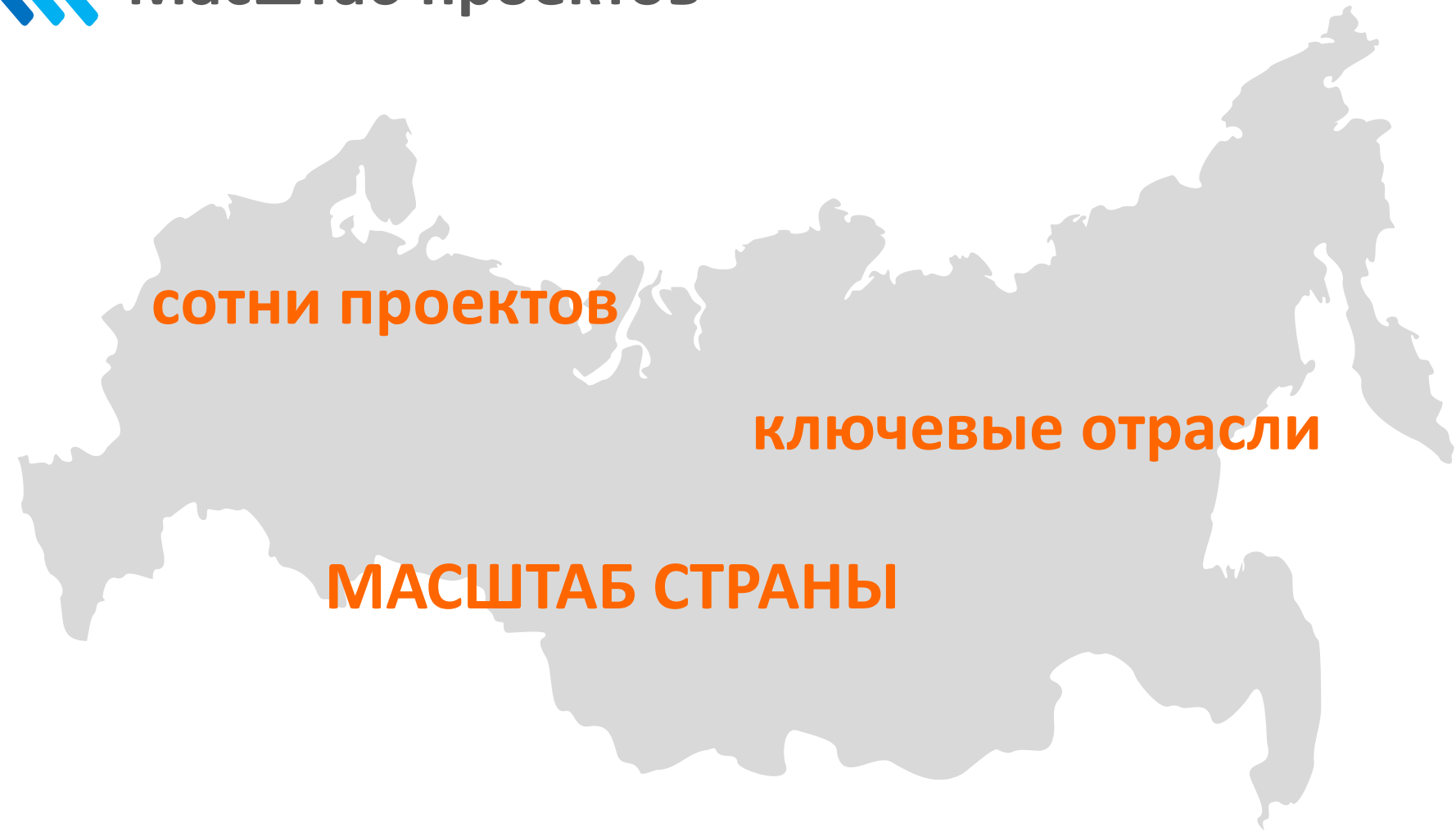
Основные виды деятельности:

- Реализация крупномасштабных интеграционных проектов по созданию защищённых информационных систем.
- Консалтинг в области построения защищённых информационных систем, включая проектный консалтинг и аттестацию объектов информатизации.

Наши клиенты

Ведущие крупные российские компании из **ФИНАНСОВОГО СЕКТОРА**, энергетики, ГАЗО- И НЕФТЯНОЙ НЕФТЕДОБЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ, ТЕЛЕКОММУНИКАЦИОННОЙ ОТРАСЛИ, предприятия оборонного комплекса, **региональные и федеральные органы власти**, ГОСУДАРСТВЕННЫЕ УЧРЕЖДЕНИЯ И ОРГАНИЗАЦИИ

Масштаб проектов



От корпоративной «мобильности» никуда не денешься

>70%

регулярно используют личные мобильные устройства для выполнения служебных функций

Право или привелегия?

>50%

считают такое использование личных мобильных устройств своим правом, а не привилегией

Откуда ноги растут?

1. Тренд, модно.
2. Удобно, выгодно.
3. Эффективно.

Что дает концепция BYOD

Концепция, посредством которой сотрудникам компании предоставляется возможность использовать собственные мобильные устройства для выполнения служебных обязанностей

В чем выгода? Общее мение.

Для компании

1. Увеличение продуктивности сотрудника.
2. Экономия на средствах связи для сотрудника.
3. Мобильность и доступность сотрудника.
4. Лояльность сотрудника.

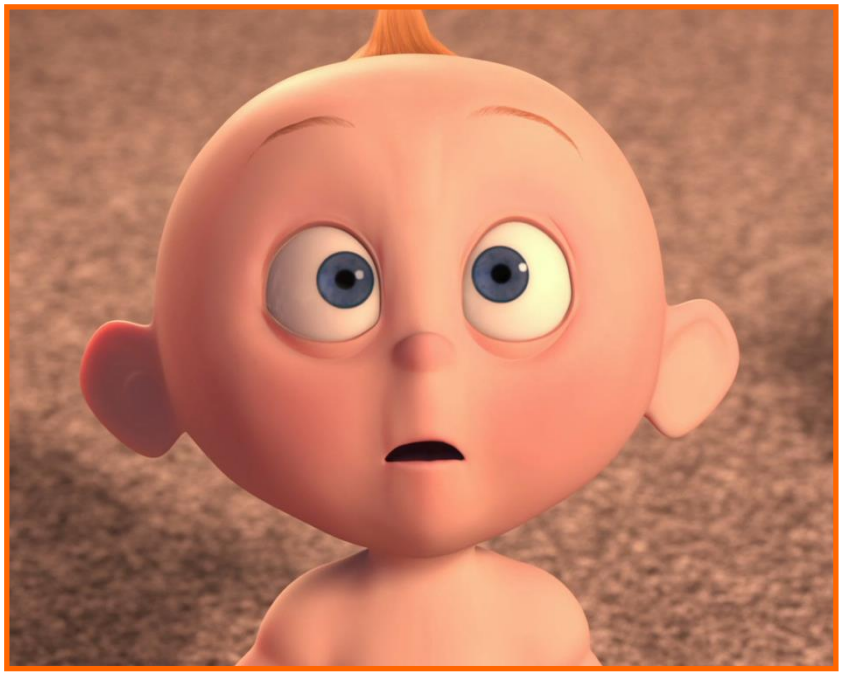
Для сотрудника

1. Право выбора личного устройства.
2. Независимость от корпоративных стандартов.
3. Мобильность сотрудника.
4. Баланс между личной жизнью и работой.

Возможные проблемы, связанные с концепцией BYOD, глазами компании

1. Кража, утеря мобильных устройств пользователями.
2. Несанкционированный доступ в корпоративную сеть с помощью украденного/потерянного мобильного устройства.
3. Утечка конфиденциальной (кража данных) информации через потерянные устройства.
4. «Внедрение» через мобильные устройства в корпоративную сеть вредоносного программного обеспечения.
5. Прочие угрозы.

Проблемы, связанные с концепцией BYOD, глазами сотрудника



Ммм, проблемы?

Нужен компромисс, баланс интересов

В чем может быть компромисс

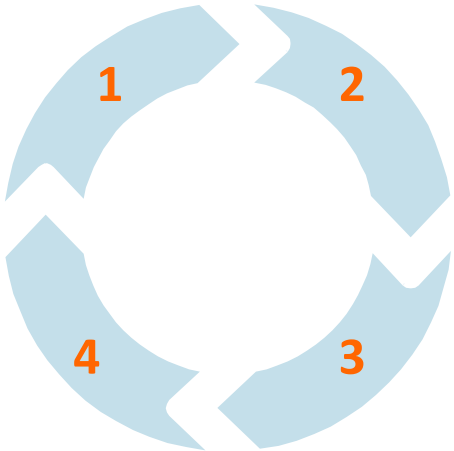
!

1. Для **компании**: подготовка и реализация единой политики безопасности для мобильных устройств.
2. Для **сотрудника**: гибкость политики безопасности.

Политика безопасности для мобильных устройств

Планирование и организация

Организационные мероприятия



Реализация технических мер

Учет правовых аспектов

Планирование и организация

1. Ответить на вопрос – насколько BYOD необходим компании и какие бизнес задачи будут решаться?
2. Узнать отношение сотрудников компании к BYOD.
3. Выявить возможные угрозы и риски связанные с BYOD.
4. Уточнить – требуется ли соответствие требованиям регуляторов?
5. Определить, возможно ли интеграция политики безопасности BYOD в существующую ИТ и ИБ концепцию компании.
6. Прочее.

Организационные мероприятия

1. Разработка регламентирующих документов, например:
   - Регламент безопасного подключения мобильных устройств.
   - Регламент обмена и хранения данных.
   - Регламент управления приложениями.
2. Определить перечень мобильных устройств/платформ.
3. Проработка алгоритма действий в случае кражи/утери мобильного устройства.
4. Проработка порядка реагирования на инциденты.
5. Прочее.

Правовые аспекты

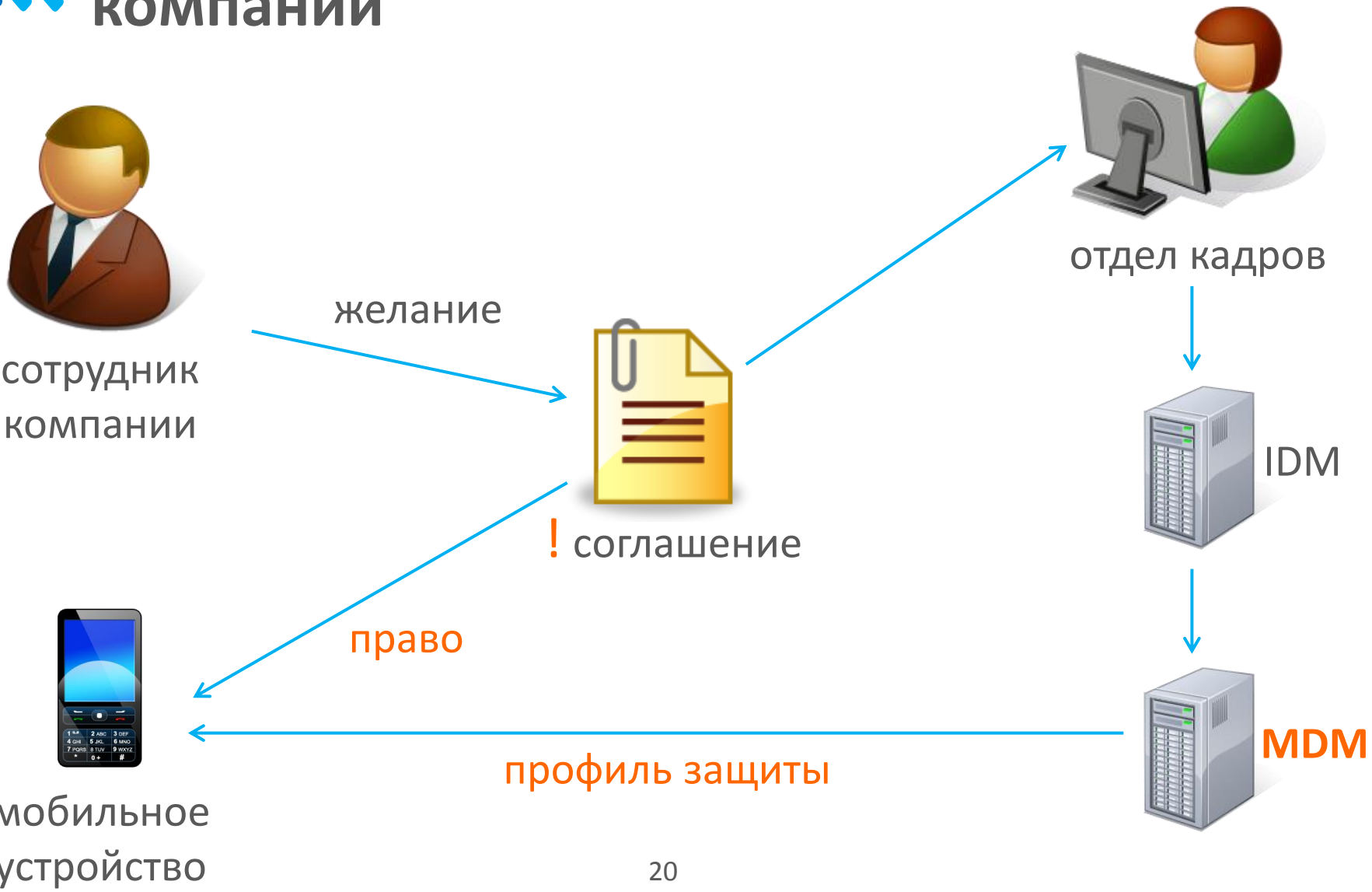
«Узаконить» право пользования мобильными устройствами в компании:

- Заключить доп. соглашение с сотрудником.
- Определить порядок увольнения сотрудника и «лишения» его прав на мобильный доступ.
- Согласовать, как будет осуществляться мониторинг и отслеживание за мобильным устройство сотрудника.
- Прочее.

Технические меры

1. Выбор технических средств – MDM.
2. Разработка корпоративной политики доступа:
   - Правила доступа из/вне контура компании.
   - Правила шифрования – VPN, крипто-контейнеры.
   - Усиленная аутентификация при доступе к ресурсам.
   - Перечень корпоративных ресурсов – e-mail, календарь, документы, др.
   - Антивирусная защита.
   - Удаленной управление устройством, принудительное удаление информации на устройстве.
   - Прочее.

Пример реализации сценария MDM в компании



Профиль защиты

1. VPN.
2. Электронная почта.
3. Календарь.
4. Возможность удаленного управления мобильным устройство.

Вывод

1. Сегодня, запретить пользоваться мобильными устройствами в компании практически невозможно.
2. Принимать риски, связанные с мобильными устройствами или управлять ими – право каждой отдельной компании.
3. В реализации безопасного BYOD главное не «перегибать» палку и извлекать для себя выгоду.

www.elvis.ru

Лунгу Максим Аурелович
Начальник Отдела решений по контролю и защите контента
e-mail: lungu@elvis.ru
Тел. рабочий: (495) 276-0211, 424
Тел. моб.: 8 (916) 933-02-40