



СБЕРБАНК

Всегда рядом

Управление корпоративными и личными мобильными устройствами

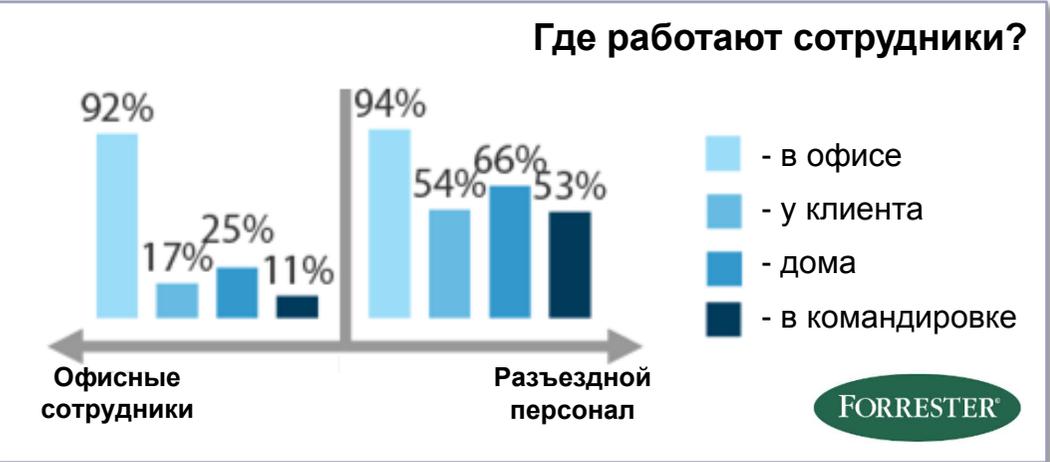
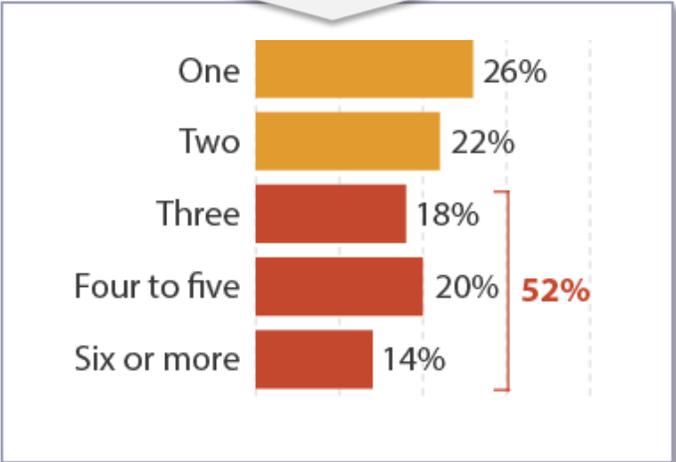
Сизов Алексей

Управление развития архитектуры ИТ

октябрь 2015 г.

60% офисных работников используют мобильные устройства для рабочих и личных целей.

52% офисных работника используют несколько различных устройств в рабочих целях.



Современный мир стирает границы между работой и личной жизнью. 67 % людей, использующих смартфоны для работы, и 70 % тех, кто использует для работы планшеты, выбирают устройства сами, не всегда задумываясь о том, сможет ли их компания обеспечить соответствующую поддержку.

Количественные выгоды (время):

- Повышение скорости реакции сотрудников на различные инциденты; своевременная выработка корректирующих воздействий;
- Ускорение бизнес-процессов за счет более плотной вовлеченности всех сотрудников.

Качественные выгоды (гибкость):

- Повышение гибкости и отлаженности работы системы;
- Оптимизация баланса работы и частной жизни сотрудников;
- Сокращение времени реагирования на запросы



Выгоды и затраты:

Продуктивность сотрудников

+12%

Звонки в Help Desk

+8%

Стоимость замены устройств

-15%

Обеспечение безопасности

+7%

Стоимость доступа к данным

-8%

Дополнительное оборудование

+3%

FORRESTER

Использование мобильных устройств

Роли:

Руководители

Эффективное управление:

- Оперативно узнавать о проблемах и реагировать на события.
- Ставить поручения и контролировать их исполнение.
- Оперативный доступ к отчетам и аналитическим материалам в online и offline.

Разъездной персонал

Эффективная работа:

- Быстрый доступ к корпоративным приложениям в любом месте (в том числе и у клиента).
- Мониторинг передвижения персонала и контроль за их результатами в реальном времени.

Офисные сотрудники

Эффективные коммуникации:

- Простота доступа к корпоративной информации.
- Связь с коллегами в любое время суток и в любом месте.

Корпоративная мобильная платформа



1

Аналитика и отчетность

- Информация о состоянии компании «на одной странице»
- Корпоративная отчетность
- Бюджетирование
- Новости
- Котировки.



2

Бизнес приложения

- Электронный документооборот и согласование.
- Каталог продуктов.
- Планирование продаж и контроль результатов.
- Контроль за передвижением разъездного персонала.



3

Мобильный офис

- Корпоративная почта.
- Календари.
- Обмен сообщениями.
- Защищенный файловый ресурс.
- Управление задачами.

Риски и проблемы

Пользователи:

Руководители

Разъездной персонал

Офисные сотрудники

Приложения:



Аналитика и отчетность



Бизнес приложения



Мобильный офис

Безопасность



Управление

Основные **риски**, связанные с мобильными устройствами:

- Утеря либо кража устройства
- Взлом устройства через сетевые подключения
- Взлом устройства через уязвимости в используемом ПО
- Утечка информации из-за заражения вредоносным ПО
- Перехват трафика от и до устройства
- Похищение учетных данных пользователя для доступа к корпоративным сервисам.

Основные **проблемы** управления мобильными устройствами и корпоративными приложениями:

- Большое количество типов мобильных устройств от разных производителей.
- Сложность дистанционного администрирования мобильных устройств.
- Сложность своевременного обновления корпоративного ПО.
- Сложность дистанционного распространения корпоративных мобильных приложений.



← Контроль за устройством

Нет вмешательства в устройство →

Обеспечение безопасности устройства:

- Контроль целостности платформы
- Управление политиками безопасности
- Шифрование данных
- Управление **всеми** приложениями

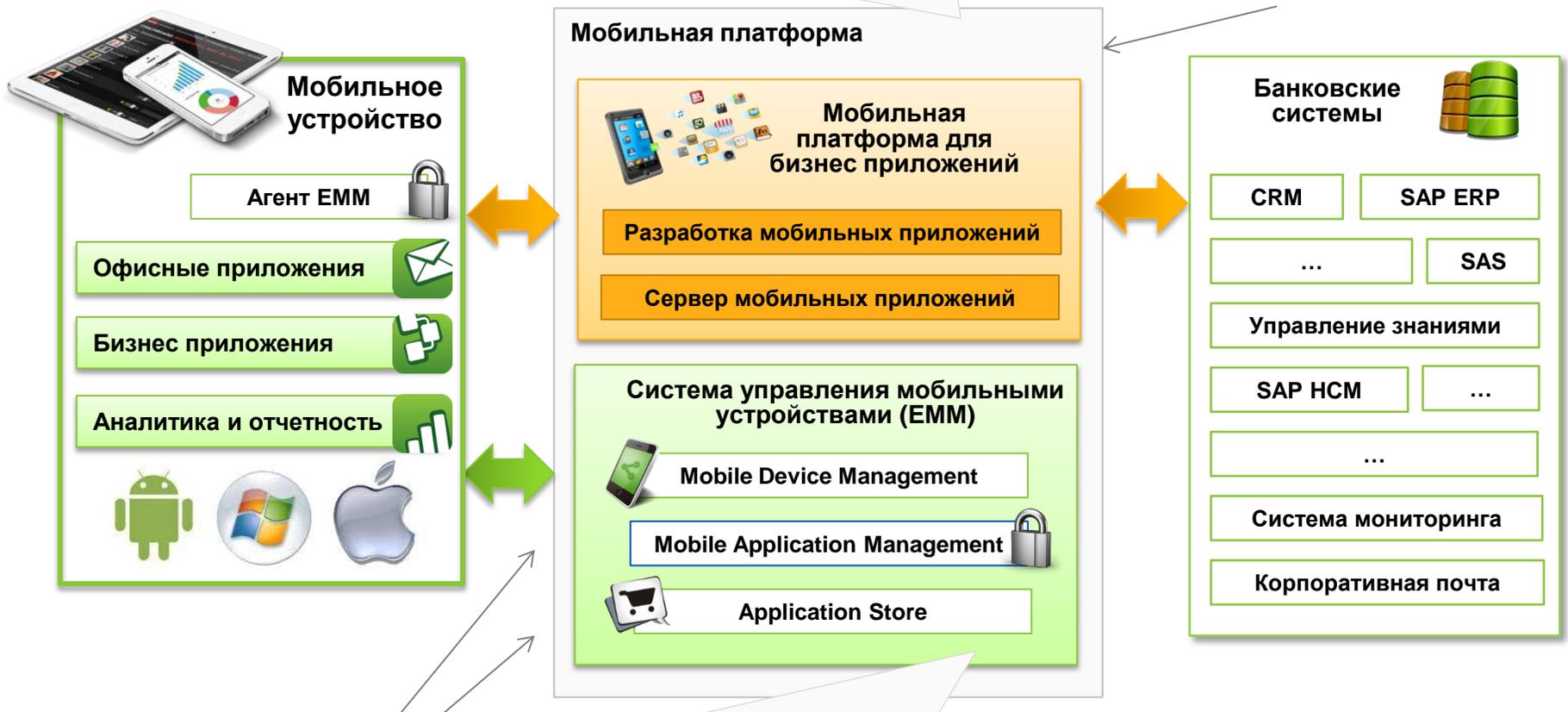
Обеспечение безопасности данных:

- Обеспечение безопасности отдельных приложений.
- Управление отдельным приложением без доступа к остальным данным.

Архитектура корпоративной мобильной платформы

Платформа для разработки корпоративных мобильных решений позволяет создавать бизнес приложения для любых типов устройств и обеспечивает выполнение их бизнес логики.

Разработка и поддержка



Безопасность и управление

Система управления мобильными устройствами (EMM) обеспечивает управление доступом, возможность дистанционной конфигурации устройства и настройки параметров безопасности. Включает в себя два направления: Mobile Device Management и Mobile Application Management.

Архитектура корпоративной мобильной платформы

Платформа для разработки корпоративных мобильных решений позволяет создавать бизнес приложения для любых типов устройств и обеспечивает выполнение их бизнес логики.

Разработка и поддержка



Безопасность и управление

Система управления мобильными устройствами (EMM) обеспечивает управление доступом, возможность дистанционной конфигурации устройства и настройки параметров безопасности. Включает в себя два направления: Mobile Device Management и Mobile Application Management.

Управление мобильными устройствами Enterprise Mobile Management (EMM)

Mobile Device Management - система, которая обеспечивает ролевое управление доступом, возможность конфигурации и обеспечения безопасности мобильных устройств на уровне устройства в целом.

Mobile Application Management — защита и управление на уровне отдельных приложений. Этими приложениями может управлять администратор, не имеющий доступа к устройству в целом и личной информации владельца.



Мобильное устройство

Агент EMM



Офисные приложения



Бизнес приложения



Аналитика и отчетность



Управление:

- Установка приложений
- Настройка приложений
- Обновление приложений
- Контроль использования

Безопасность:

- Назначение политик безопасности
- Контроль целостности
- Шифрование данных
- Дистанционная очистка устройств.

**Система управления
мобильными устройствами
(EMM)**

Mobile Device Management



Application Management



Enterprise Application Store



Основные функции системы управления мобильными устройствами (EMM).

- Установка сертификатов
- Настройка VPN
- Настройка подключения к корпоративному wi-fi и почте
- Доступ к рабочему столу, файловой системе и диспетчеру процессов

Администрирование мобильных устройств

- Дистанционная очистка корпоративных данных и приложений (без полной очистки устройства).
- Ограничение функционала устройств
- Контроль целостности мобильной ОС, шифрование устройства

Обеспечение информационной безопасности

Обеспечение защиты мобильных приложений

- Шифрование данные на уровне приложения.
- Политики безопасности для каждого приложения.
- Запрет на копирование информации между приложениями.
- VPN туннель для каждого приложения

Развертывание и управление приложениями.

- Дистанционное управление корпоративными приложениями
- Доставка и установка сертификата безопасности Наличие необходимых API для мобильных приложений
- Магазин корпоративных приложений

 - Mobile Application Management

 Mobile Device Management



Корпоративные мобильные устройства

Корпоративные мобильные устройства закупаются Банком. В корпоративном мобильном устройстве должно быть установлено только доверенное ПО, а само устройство должно быть **подключено к централизованной системе управления мобильными устройствами (Mobile Device Management)**.

- ✓ Унификация типов устройств для упрощения управления.
- ✓ Доступ к любым мобильным корпоративным приложениям в соответствии с ролями.
- ✓ Обеспечение максимального уровня информационной безопасности.

Бизнес приложения



Бизнес приложения



Аналитика и отчетность



Личный кабинет



Личные мобильные устройства

Использование личных мобильных устройств в соответствии с принципами **Bring Your Own Device (BYOD)**, для подключения к корпоративным ресурсам. Предполагает ограниченный набор использования корпоративных мобильных приложений в соответствии с политиками безопасности Банка.

- ✓ Простота и удобство работы с корпоративной информацией.
- ✓ Ограниченный набор корпоративных мобильных приложений.
- ✓ Обеспечение безопасности приложения за счет его контейнеризации (Wrapper).

Офисные приложения



Управление задачами



Обмен файлами



Почта
Календарь







СБЕРБАНК

Всегда рядом

Спасибо за внимание!