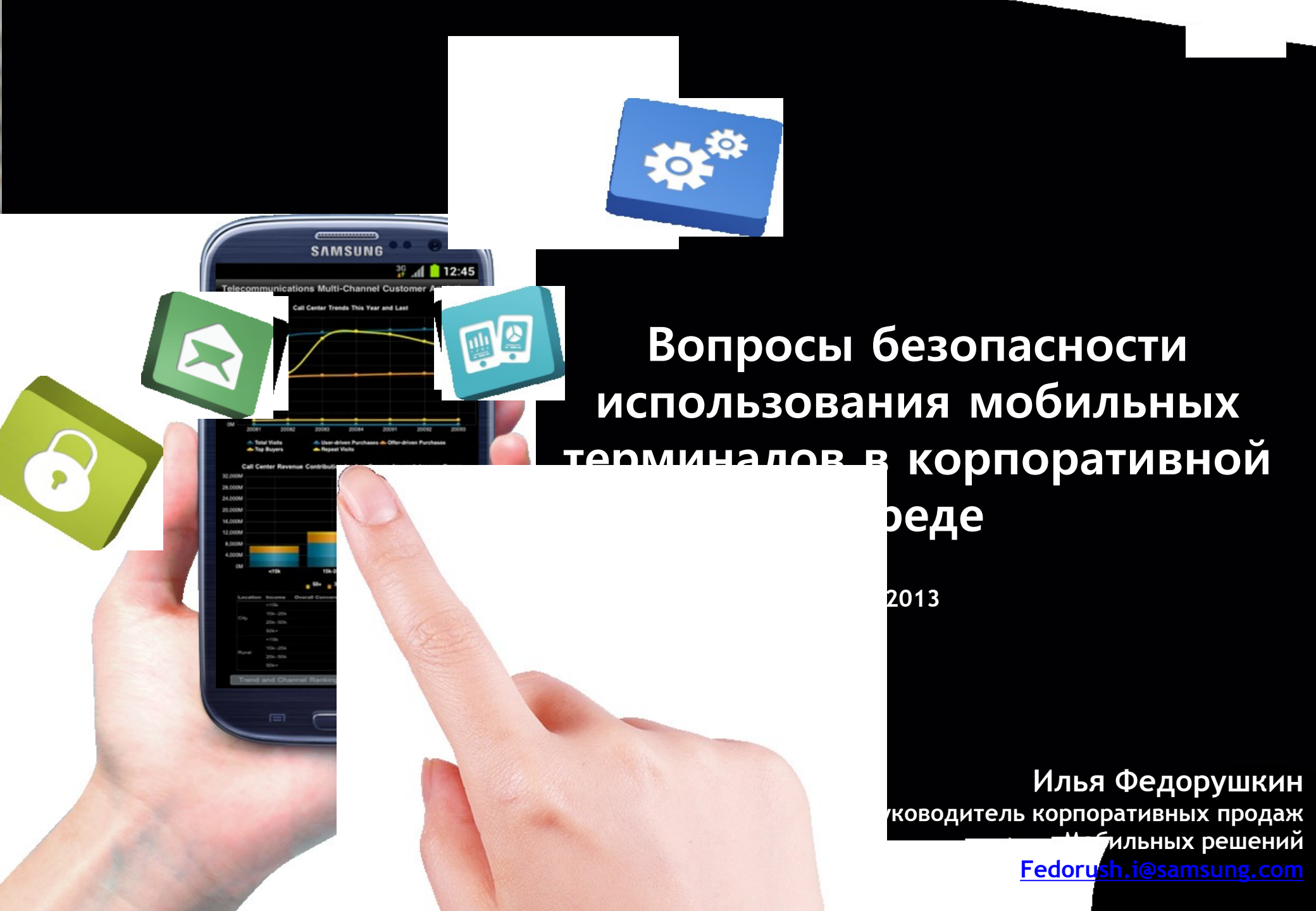




Вопросы безопасности использования мобильных терминалов в корпоративной среде

2013

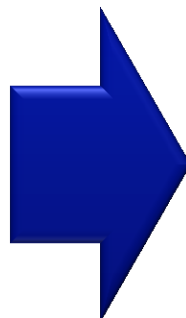
Илья Федорушкин
руководитель корпоративных продаж
мобильных решений

Fedorush.i@samsung.com

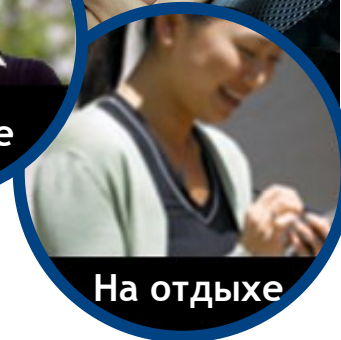
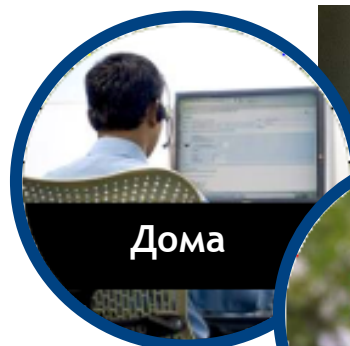
Прогноз: Что день грядущий нам готовит?

Меняется подход к рабочему процессу

Рабочие часы



Рабочие минуты



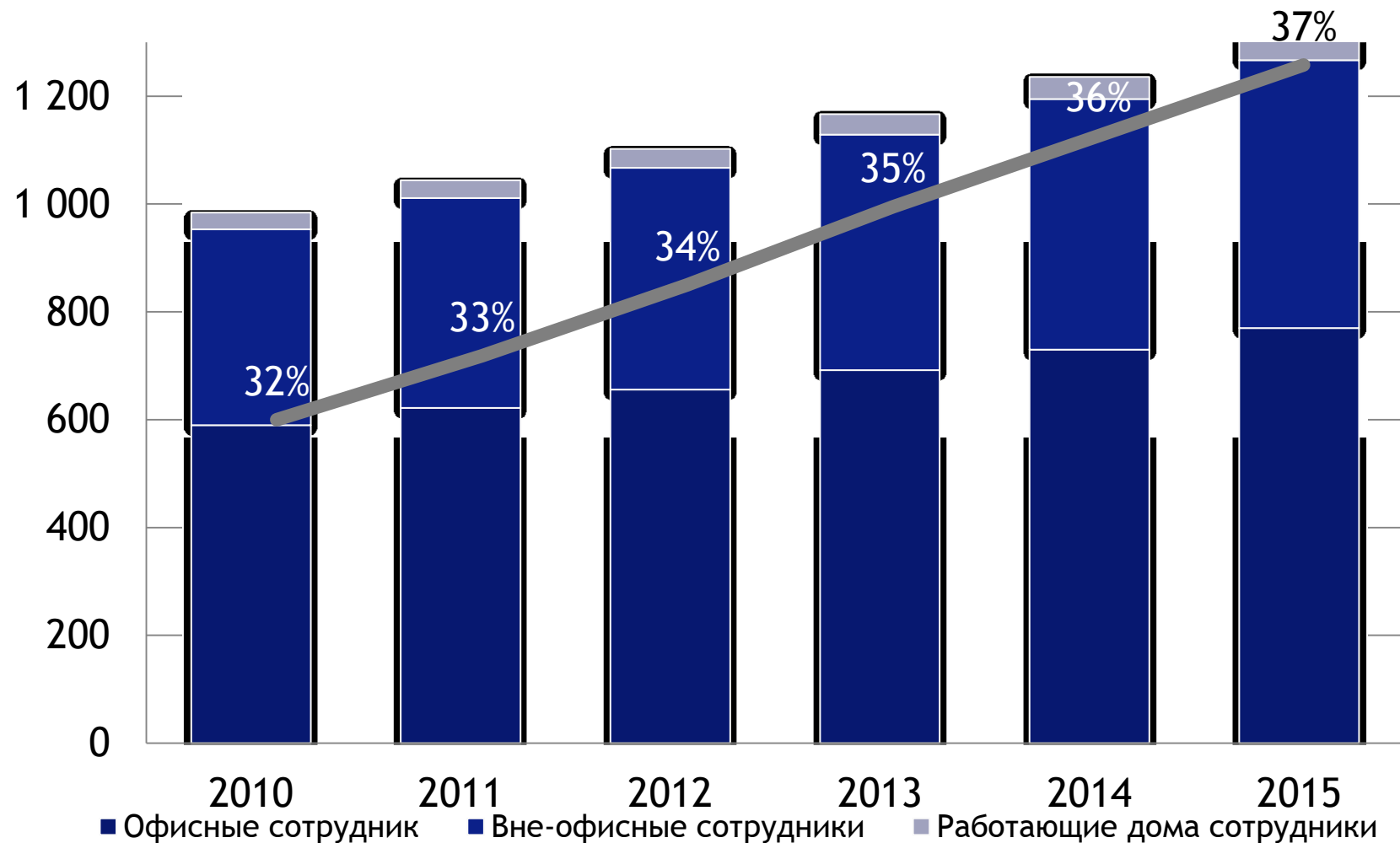
ПРОЦЕСС => РЕЗУЛЬТАТ

- Минуты «максимальной эффективности»
- Непрерывный рабочий процесс
- Гибкий баланс работа – личная жизнь



Прогноз: Количество мобильных сотрудников в мире

Исследование IDC в 2012 году (WW)



□ % мобильных сотрудников от всего работающего населения

Что день грядущий нам готовит: Смена парадигмы

Традиционный ПК



Традиционный монитор

Кабель
подключения
монитора



ПК

Виртуальный десктоп



«Облачный» монитор

Сетевой
кабель



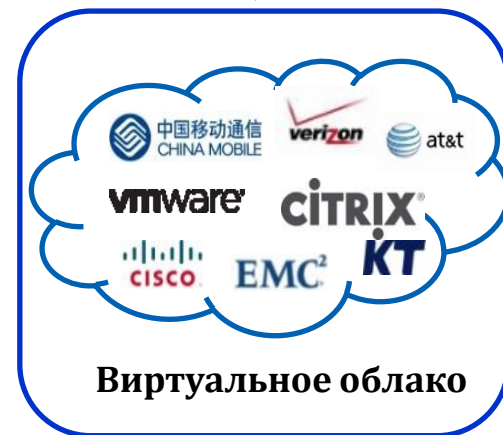
Планшет, смартфон



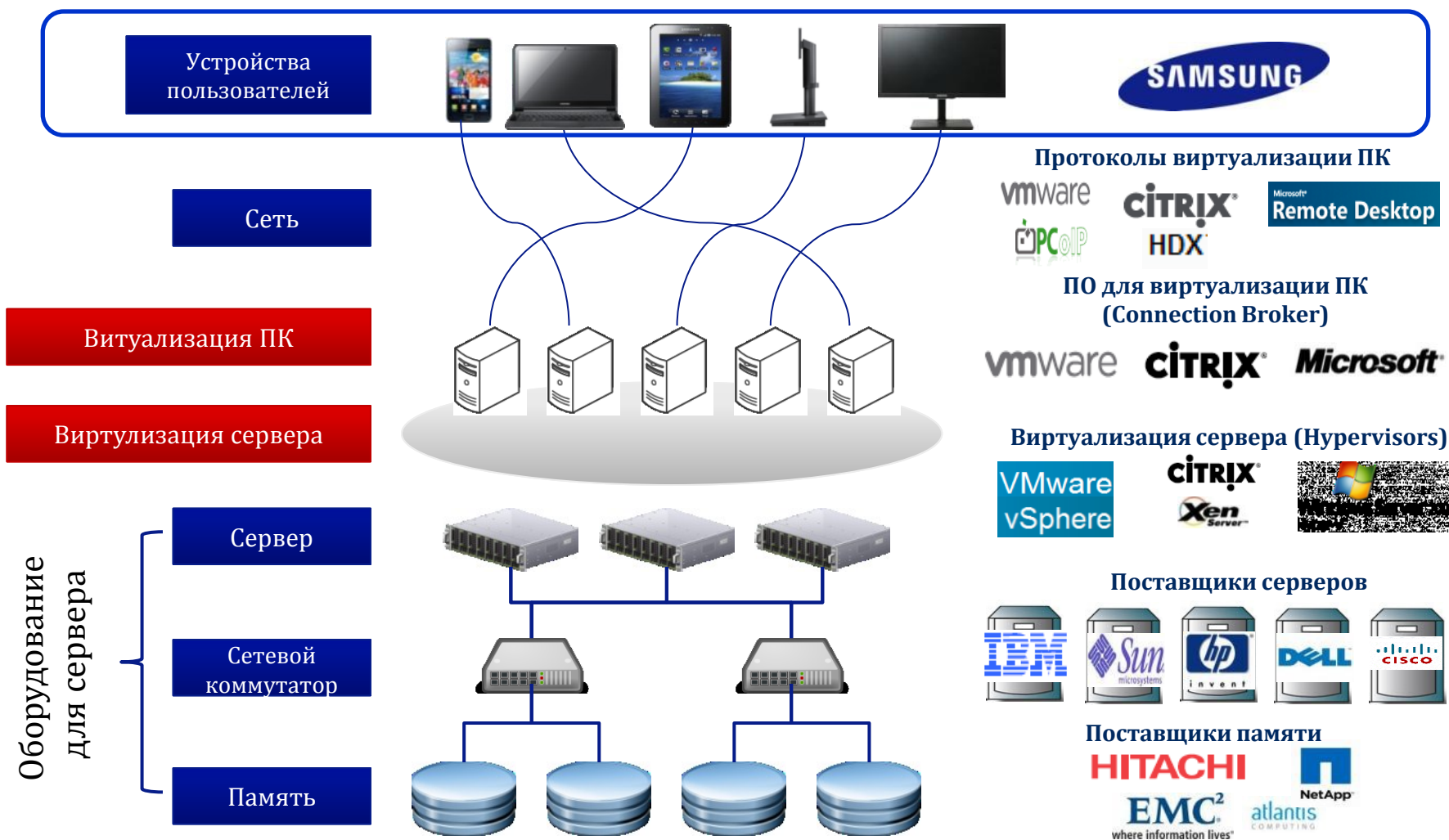
Мобильные устройства



LTE, Wi-Fi, 3G



Экосистема: требуется защита на всех уровнях



Риски использования мобильных устройств



Небезопасно!

Нефункционально!

Неудобно!

БЕЗОПАСНОСТЬ

- ✓ потеря и кража устройств
- ✓ утечка данных
- ✓ платный тарифик/контент
- ✓ неавторизованный доступ к корпоративным ресурсам
- ✓ передача вредоносного ПО с мобильных устройств на корпоративную сеть
- ✓ нарушение политик безопасности

Выбор: подготовительная работа



- Цели, основные требования внутренних заказчиков, ROI
 - ✓ Цели: В большинстве случаев это повышение производительности труда сотрудников
 - ✓ Требования: Баланс удобство/безопасность, набор корпоративных инструментов, работа в любое время / в любом месте
 - ✓ ROI: Расчет экономического эффекта - повышение производительности + сокращение расходов против затрат на решение, корпоративные устройства / BYOD

Пример

	Стационарный	Мобильный
Доход от сотрудника (мес)	\$50.000	\$55.000
Затраты на 5 кв.м. Офиса (мес)	\$100	\$80
Эл-во, прочие затраты (мес)	\$10	\$8
Терминал, мебель	\$1100	\$1080
ПО для обеспечения мобильного сотрудника	\$0	\$200
ИТОГО (экономия)		
Единоразово	-\$180	
Ежемесячно	\$5022	

Выбор: проработка концепции



- Поддерживаемые операционные системы
С учетом их достоинств и недостатков
- Определение групп пользователей
 - ✓ Совместно с руководителями подразделений, кадровыми службами необходимо определить спектр сотрудников, которым буде предоставлена возможность удаленной работы.
 - ✓ Разделение на группы в зависимости от набора требований
- Политики
 - ✓ Совместно службами ИТ и ИБ определяются ИТ и ИБ политики для выявленных групп сотрудников и возможность ее реализации.
- Подготовка персонала
 - ✓ Повышение квалификации мобильных работников.
 - ✓ Подготовка ИТ/ИБ-персонала

Обязательно: что нужно учесть?



- Безопасный обмен между сетью организации и терминалом
- Шифрование данных на устройстве
 - ✓ Шифрование файлов
 - ✓ Шифрование внешних носителей
 - ✓ Запись только зашифрованных файлов на внешние носители
- Безопасная среда для приложений
 - ✓ Все мобильное устройство
 - ✓ Изолированная среда («песочница»)
- Контролируемый пул приложений
Создание корпоративного «магазина» приложений
- Фильтрация контента
- Прозрачность управления мобильной платформой
- Соответствие требованиям регулятора

Политики (до 338): в зависимости от требований компании



- ✓ Удаленная блокировка/разблокировка устройства
- ✓ Стирание информации с устройства (сброс к заводской конфигурации)
- ✓ Выборочное стирание информации (например, почта)
- ✓ Управление парольной политикой и основным функционалом операционной системы самого устройства
- ✓ Определение месторасположения устройства, трекинг
- ✓ Домашняя страничка пользователя (с возможностью заблокировать/разблокировать, найти свое устройство, а также просмотреть статистику по его использованию)

- ✓ Контроль приложений
- ✓ Настройка доступа к Exchange, централизованное использование его политик
- ✓ Блокировка доступа к электронной почте из сторонних приложений
- ✓ Настройка доступа к сетям WiFi
- ✓ Настройка VPN
- ✓ Создание резервных копий информации с устройства/восстановление файлов
- ✓ Сбор статистики о входящих и исходящих звонках/SMS
- ✓ Копирование контактной информации между терминалом и облаком

Политики: влияние на угрозы

	Потеря/ кража устр-ва	Платный контент/ трафик	Утечка данных	Доступ к ресурсам	Вредо- носное ПО	Нарушение правил/ политик
Удаленная блокировка/разблокировка устройства	+		+	+		+
Стирание информации с устройства (сброс к заводской конфигурации)	+		+	+	+	
Выборочное стирание информации (например, почта)	+		+		+	
Управление парольной политикой и основным функционалом операционной системы	+	+	+	+	+	+
Определение месторасположения устройства, трекинг	+	+				+
Домашняя страничка пользователя (заблокировать/разблокировать, найти, статистика)	+		+	+	+	
Контроль приложений		+	+	+	+	+
Настройка доступа к Exchange, централизованное использование его политик			+	+		+
Блокировка доступа к электронной почте из сторонних приложений		+	+	+	+	+
Настройка доступа к сетям WiFi		+	+	+	+	+
Настройка VPN			+	+		+
Создание резервных копий информации с устройства/восстановление файлов	+		+		+	
Управление списками, сбор статистики о входящих и исходящих звонках/SMS		+			+	+
Управление разрешениями в роуминге		+				+
Управление антивирусным ПО		+	+	+	+	

Gartner:

К 2014 году 90% компаний будут поддерживать корпоративные приложения на устройствах, которые находятся в собственности работников

The Gartner logo, consisting of the word "Gartner" in a bold, blue, sans-serif font, with a small registered trademark symbol (®) to the upper right of the letter "r".

Gartner: "Внедрение пользовательских устройств (смартфонов и планшетов) в корпоративные ИТ-системы будет самым значительным трендом, влияющим на ИТ в ближайшие 10 лет".

"Основные отрасли – финансы и страхование, так как в них работает наибольшее количество мобильных сотрудников".

Рабочий и персональный образ на одном мобильном устройстве

Функции

- Установка **второй OS как приложения** на существующей OS
- Создание **двух номерных/дата планов на одном устр-ве**
- Контроль второй OS управляющим сервером
- Личный профайл на первой OS и рабочий на второй



Преимущества

- Безопасность: две изолированные среды
- Конфигурация корпоративного профайла в соответствии с требованиями IT
- Увеличение ARPU (два тарифных плана ПД на одном устройстве)
- Развитие новых услуг на Платформе Виртуализации
- Баланс работа-жизнь
- Раздельное хранение данных



Компания



Оператор



Пользователь

А безопасен ли Android?

Samsung Android - это уже не просто Android

Разработан для обеспечения высокого уровня
Информационной Безопасности



Сервисные центры
в **142** городах
России

SAMSUNG ориентируется на компании

300+ B2B сотрудников R&D работали более 3х лет



Обеспечение безопасности: Мобильные устройства

Поддержка **EAS** политик (40) и расширенная поддержка **e-mail, контактов и синхронизации календаря (31)**



Corporate Email
Calendar
Contacts

SW&HW On Device Encryption (AES-256 bit) защищает от несанкционированного доступа к данным, включая **microSD®**



On Device
Encryption



Интеграция с VPN с поддержкой **IP-шифрования** для доступа в корпоративную сеть (включая ГОСТ)

Virtual
Private Network

Mobile Device
Management

338
IT-политик



Гибкое и масштабируемое **управление мобильной средой**.
Поддержка политик и он-лайн управления.

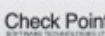
Мобильное устройство - часть экосистемы

Обязательное условие – интеграция с ведущими производителями решений

Security

• VPN (Virtual Private Network)

SSL Layer 3 VPN



IPSec VPN



• MDM (Mobile Device Management)



Российские партнеры



Messaging



Novell

Microsoft

Collaboration



Virtualization



Biz App

Microsoft



Спасибо!



Илья Федорушкин
Руководитель корпоративных продаж
Мобильных решений
Fedorush.i@samsung.com