Корпоративная Мобильная Безопасность

Дастан Динасылов

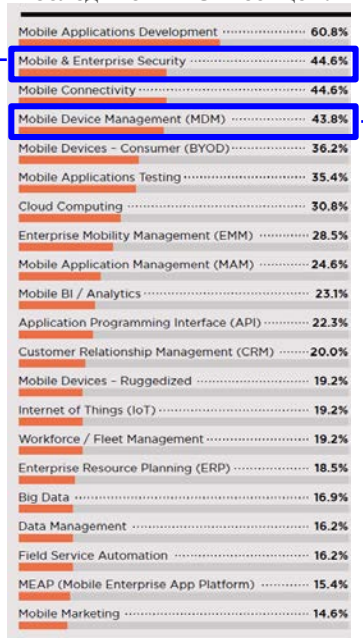
B2B IT and Mobile
Pre-sales /PM manager
Samsung Electronics

Андроид представляет риск для предприятий

- Вредоносное ПО
- Рут устройства
- Кража устройства
- Модификации Ядра
- Джус-джекинг

Важными звеньями при разработке Корпоративной Мобильности являются Безопасность и Управление

B) В какие мобильные решения Вы инвестировали за последние 12-18 месяцев?



Мобильная и Корпоративная Безопасность

44.6%

Управление Мобильными Устройствами

43.8%

* Инвестиции в Корпоративную Мобильность 2016

Каковы основные вызовы для принятия мобильности ?

Топ 3 опасения для использования Android на предприятии

Отсутствие безопасности платформы

01

Отсутствие информационной безопасности

02

Отсутствие политики контроля и управления

03

Решения Knox

Корпоративные мобильные решения, основанные на встроенной платформе

Knox Workspace

Полнофункциональный рабочий контейнер для предприятий

Knox Manage

Облачное решение по управлению устройствами EMM

Knox Configure

Набор инструментов по кастомизации и настройке

Платформа Knox

Встроенная аппаратная платформа безопасности и управления Samsung

1. Платформа Knox

Безопасность: Устройство + Информация

I. Безопасные устройства – Безопасная/Надежная Загрузка / TIMA*
II. Безопасные данные – Аппаратное шифрование (AES 256)
III. Безопасные приложения – Контейнер Knox

Усиленная безопасность от аппаратного уровня до уровня приложений

Защита в режиме реального времени с момента включения

* Архитектура определения целостности, основанная на использовании ARM TrustZone (TIMA)

Безопасность мирового класса

КАНАДА

FIPS 140-2

ВЕЛИКОБРИТАНИЯ

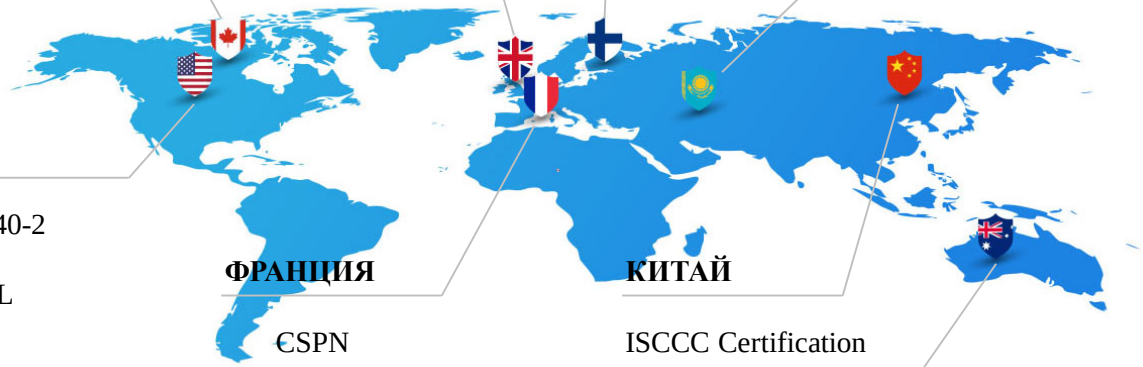
EUD Security Guidance

ФИНЛЯНДИЯ

KATAKRI II & III

КАЗАХСТАН

ST RK 1073-2007



США

FIPS 140-2
STIG
UC APL
CSFC

ФРАНЦИЯ

CSPN

КИТАЙ

ISCCC Certification

АВСТРАЛИЯ

ASD-endorsed MDFPP
for unclassified

ОБЩИЕ КРИТЕРИИ

Common Criteria

Mobile Device Fundamentals Protection Profile

Стандарты безопасности в 26 странах

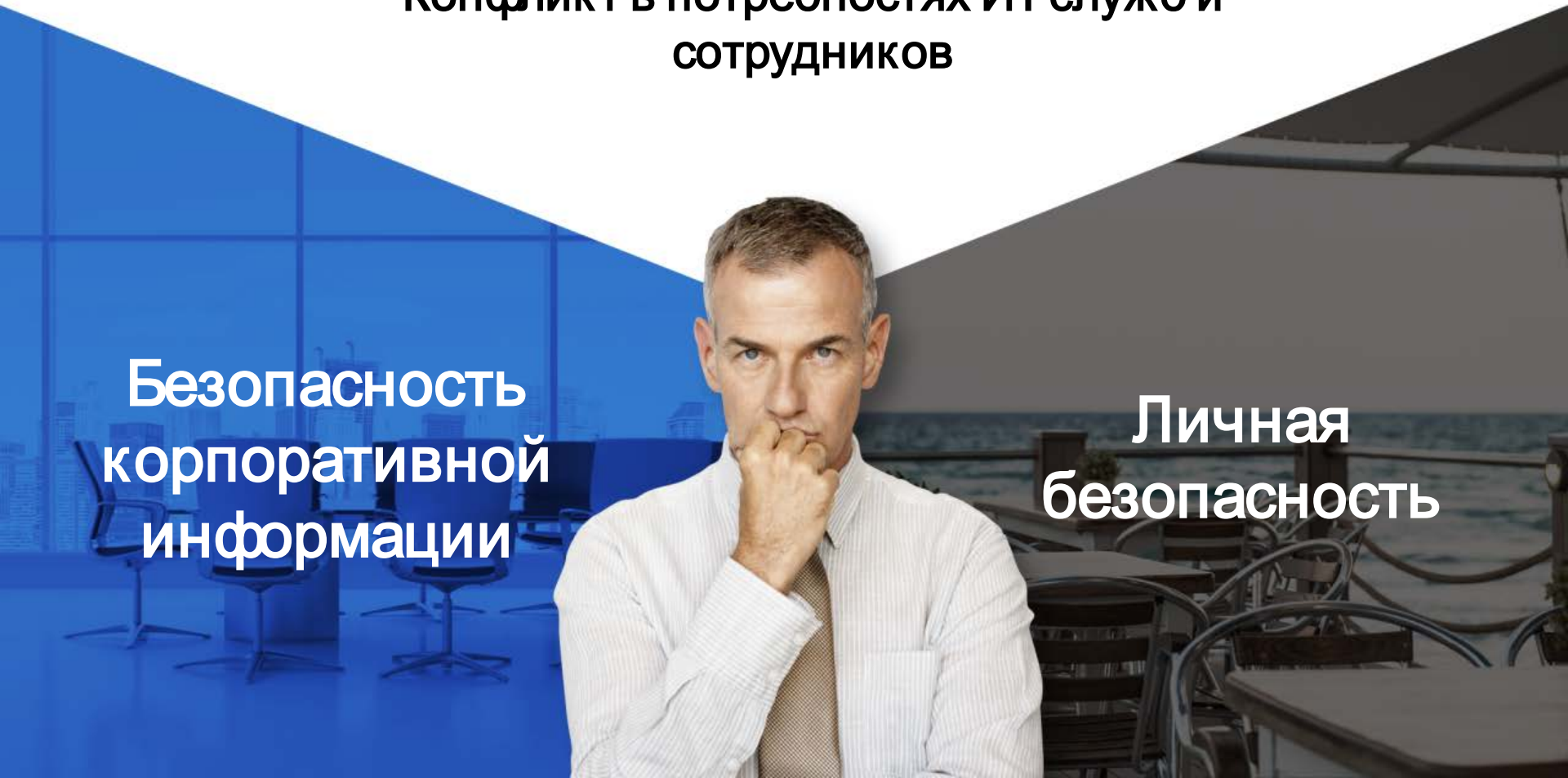
Награжден высшим баллом в области мобильной безопасности, Декабрь 2017

1ST

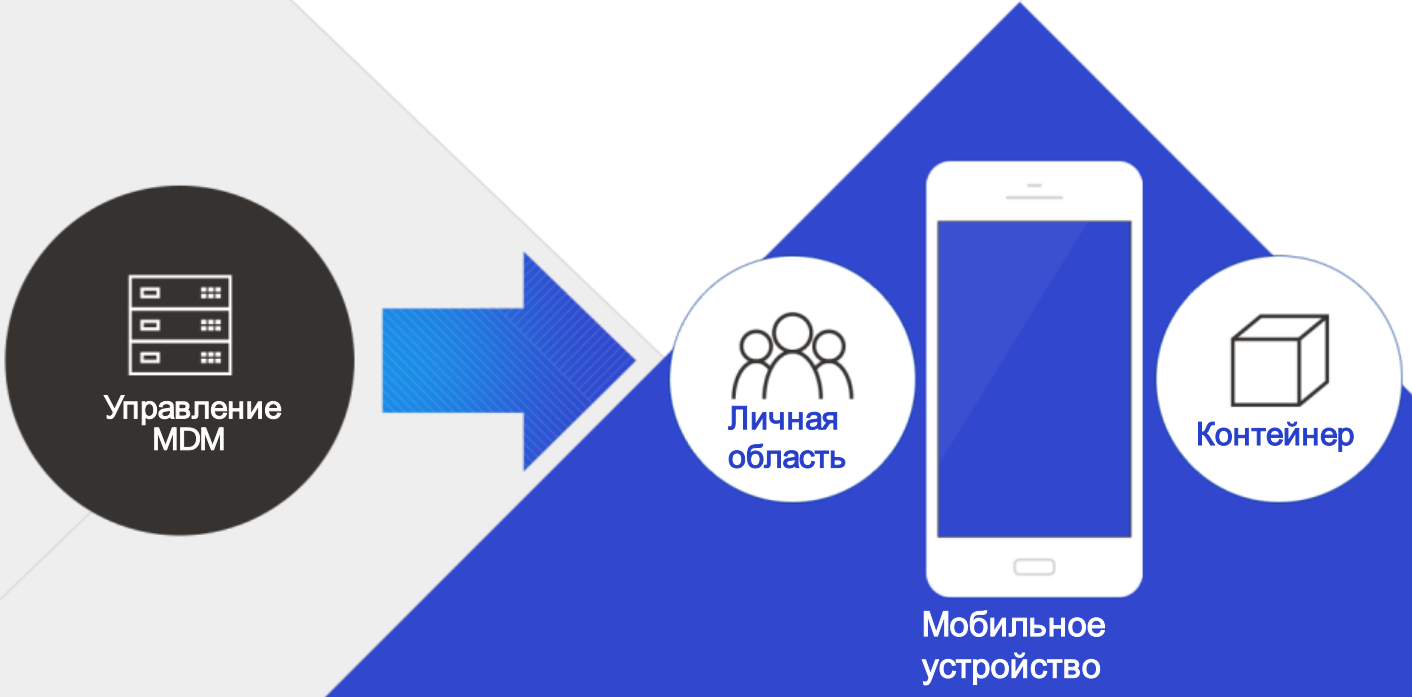
Лучшее решение по обеспечению безопасности или защиты от мошенничества

20TH GLOBAL MOBILE AWARDS

Конфликт в потребностях ИТ служб и сотрудников



Организации в настоящее время широко внедряют безопасные контейнеры



Рост угрозы безопасности

Вызов: Вирусы / вредоносные программы способны атаковать другие приложения

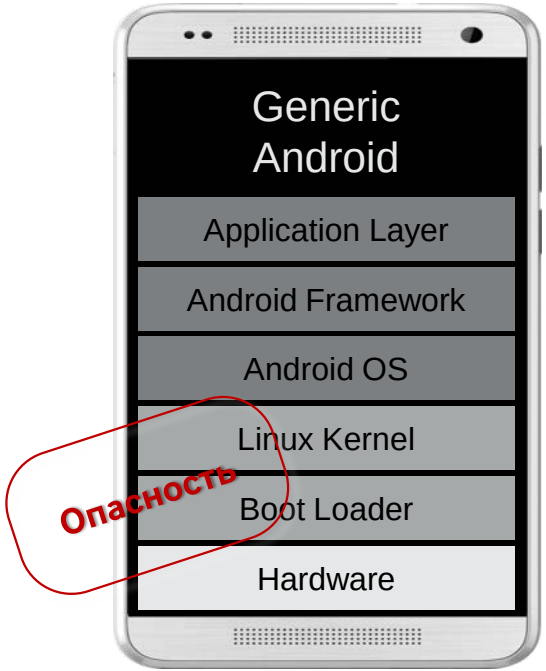
Решение: Использование антивируса или контейнерного решения защитит систему на уровне приложений.

Вызов: Что делать, если хакеры обойдут защиту на уровне приложений, получив доступ к «корневому каталогу» с помощью хакерских утилит?

Решение: Использование SE для Android не позволит хакерам делать то, что они хотят, даже если они имеют доступ к «корневому каталогу».

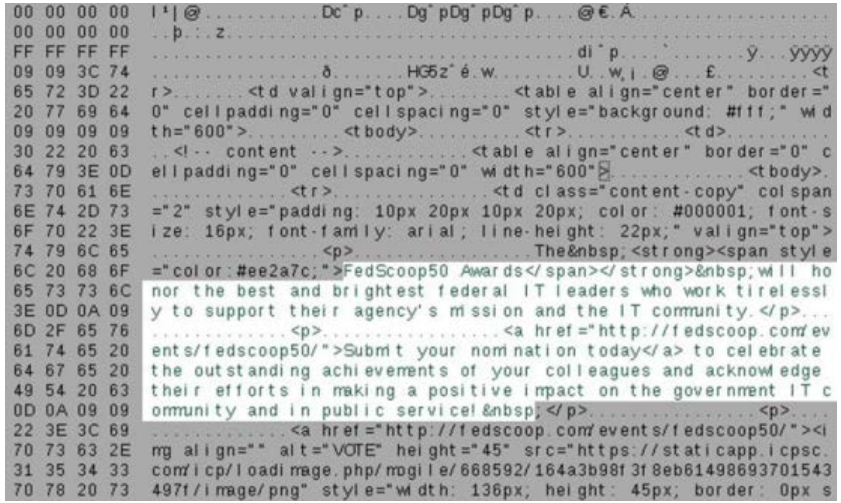
Вызов: Что делать, если хакеры отключат SE для Android с помощью хакерских утилит на уровне ядра или заменят прошивку: загрузчики и ядро Linux?

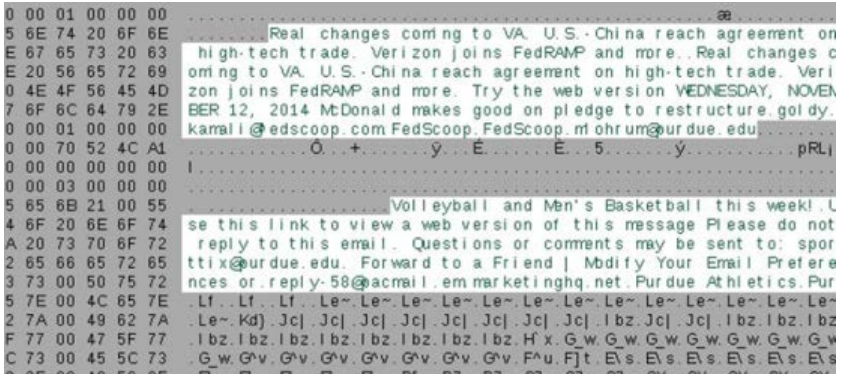
Решение: ???



Типичные векторы атаки

Сканирование RAM





Сообщение email

Полнофункциональный корпоративный контейнер

Зарекомендовавший себя на рынке:
Широко используется Банками и Гос.органами более чем в 20 странах.

Повышенная безопасность:
Защита от аппаратного уровня до уровня приложений.

Простая интеграция:
Совместимость с ведущими решениями MDM, любыми приложениями Андроид.

Усиленная безопасность приложений и данных:

- Ключ шифрования для Knox Workspace хранится в полностью изолированной аппаратной области называемой TrustZone.
- Если устройство находится под угрозой взлома, доступ к Knox Workspace заблокируется окончательно.

SAMSUNG Knox

Совместим с ведущими EMM решениями

...

- или -

SAMSUNG Knox Manage

Применение: Регулируемые отрасли

Продукты: Tab Active 2 + Knox Workspace
Цель проекта: Автоматизация работы служб министерств

Примеры использования:
- Планшеты в машинах
- Онлайн доступ к общей базе с данными о штрафах, нарушениях, налогах
- Возможность составления онлайн протокола (доступна электронная подпись)
- Авторизация по отпечатку пальца, биометрическая аутентификация
- Защита данных (Knox платформа)

Целевая аудитория:
- Дорожная полиция
- Районные полицейские
- Военные/ Армия/Силовые службы

EMM - Облачное решение по управлению и мониторингу мобильным парком устройств

Экономически выгодное решение:
Дешевле большинства существующих MDM решений

Простое управление:
Простая конфигурация устройств через веб-консоль.

Активный мониторинг устройств:
Удаленный помощник, определение местоположения.

Управление устройством с учетом конкретных событий:
Применение различных политик в зависимости от типа события (Время, Приложение, Имя сети Wi-Fi, смена сим-карты, Роуминг, Профиль-исключение по каждому пользователю)

EMM (облачный)

Управление мобильными устройствами (EMM)

MDM Сервер

Управление устройствами

Управление приложениями

Управление контентом

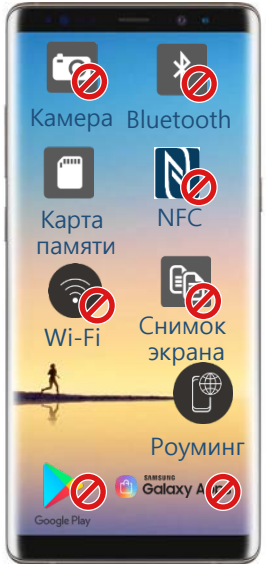
Android, iOS, Windows 10, Tizen

SAMSUNG BUSINESS

Надежная управляемость - Управление устройством с учетом конкретных событий

Контроль за устройством пользователя

- в определенное время
- при использовании роуминга пользователем за границей
- при запуске определенного приложения на устройстве
- при подключении устройства к сети Wi-Fi с определенным именем
- при установке несанкционированной SIM-карты
- при установке администратором исключающей политики для определенного пользователя на заданный интервал времени



Доступна блокировка функций и настройка разных профилей (для разных уровней)

АО «Казпочта» - сегодня

Более 4 500 000 штук ежегодно

Выданных почтовых отправлений через мобильное приложение

6 159

Почтальонов

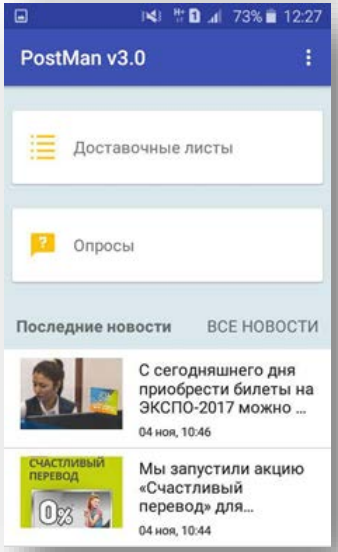
110

курьеров

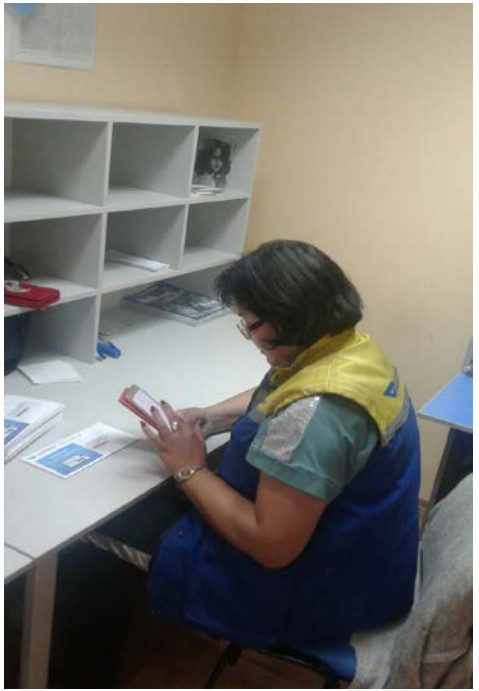
6 269

смартфонов

Возможности мобильного приложения Mobile Postman 3.0



- ✓ Автоматическое закрытие доставочных листов в системе
- ✓ Косвенные выгоды в виде экономии бумаги А4 на сумму более 40 млн. тенге в год
- ✓ В приложении запущены модули «Выдача РПО», «Новости», «Социальные опросы», «Сбор информации о социальном статусе» в приложении
- ✓ Рост обработанных почтовых отправлений с момента запуска проекта вырос почти в 300 раз

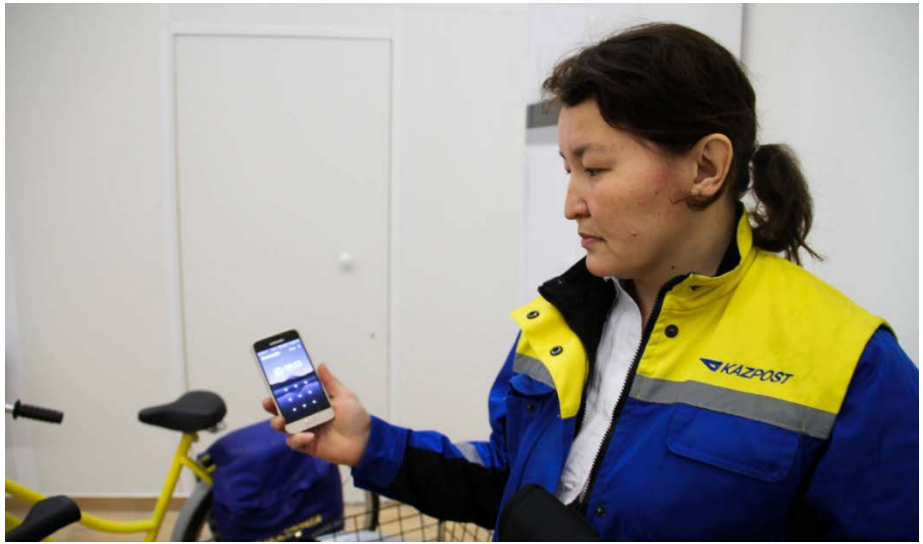


KAZPOST

О клиенте

Акционерное общество «Казпочта» - казахстанская компания, оператор казахстанской национальной почтовой сети.
Центральный аппарат - в г. Астана. Член Всемирного почтового союза, принципиальный участник международных платёжных систем *VISA International* и *MasterCard Worldwide*.

- Кол-во сотрудников: ~20 000
- Website: www.kazpost.kz



Общая информация по проекту

- **Девайсы:** Samsung Galaxy J5
- **Решение:** Knox Manage | 6 389 лицензий | срок 2 года
- **Дата завершения проекта:** Февраль 2020 года

Потребность клиента

Казпочта запустила проект «Мобильный почтальон» в 2017 году.

В рамках программы «Цифровой Казахстан» главная идея клиента - предоставить мобильное устройство с приложением каждому почтальону по всей стране.

Выгоды клиента

- Оптимизация бумажной работы почтальона: замена бумажного доставочного листа для доставки почты
- Снижение затрат и времени на первичную настройку устройств
- Возможность внедрения GPS навигации и интеграции с сортировочным центром компании (формирование маршрута)
- Автоматическая предустановка и обновление приложений
- Ограничение доступа к функционалу не связанному с работой
- Управление, контроль и удалённая помощь
- Дистанционная блокировка устройств в случае кражи/потери
- Снижение амортизации устройств
- Увеличение эффективности мобильных сотрудников

https://post.kz/info/press-centr/item/v-kazpochte-vruchili-pochtalonam-novuju-uniformu-i-smartfony

Спасибо!