

Рускрипто' 2012



конференция
РусКрипто'2012

«НАСКОЛЬКО ГЛУБОКА «ПЕСОЧНИЦА»»



НИКОЛАЙ СМИРНОВ,
ОАО «ИНФОТЕКС»



smirnovnv@infotecs.ru

© 2012, ОАО «ИнфоТеКС»

 **infotecs**[®]

План на ближайшие 20 минут



- Долгий рассказ (минут 15) о пользе и вреде навязанных систем безопасности мобильных платформ iOS и Android
- Изложение мыслей (5 минут) о пользе понимания того, кто контролирует ваше мобильное устройство, внесенное в корпоративную среду

Безопасность мобильных платформ



Изолированная экосистема

- SANDBOX
- КОНТРОЛЬ ПРИЛОЖЕНИЙ
- КОНТРОЛЬ РАЗРАБОТЧИКОВ

Безопасность мобильных платформ



SandBox

- ЭЛЕМЕНТ ВИРТУАЛИЗАЦИИ
- ПРЕДОСТАВЛЕНИЕ КОНТРОЛИРУЕМОГО ОКРУЖЕНИЯ ГОСТЕВОЙ ПРОГРАММЕ

Безопасность мобильных платформ



SandBox

- IOS
 - ЗАКРЫТАЯ ПРОПРИЕТАРНАЯ СИСТЕМА
 - ТОТАЛЬНЫЙ КОНТРОЛЬ СИЛАМИ ВЕНДОРА
- ANDROID
 - ВИРТУАЛЬНАЯ СРЕДА
 - «ТОКЕНЫ БЕЗОПАСНОСТИ» НА ПРАВО ДОСТУПА К ПОДСИСТЕМАМ



SandBox

Изолированная
среда

Доступ
приложений в
сеть и к ФС

Внешний
контроль

Контроль



Отсутствие контроля



Android

- Каждое второе приложение собирает избыточные сведения о пользователе
- Механизм запроса полномочий уязвим

iOS

- После ряда исков сбор сведений о пользователе приложениями затруднен
- Запроса полномочий нет

SandBox



Облака

iOS



Android



ДОВЕРИЕ

Доверие



Дефекты и ошибки реализации

- Ошибки есть всегда
- Любой сложный код содержит уязвимости

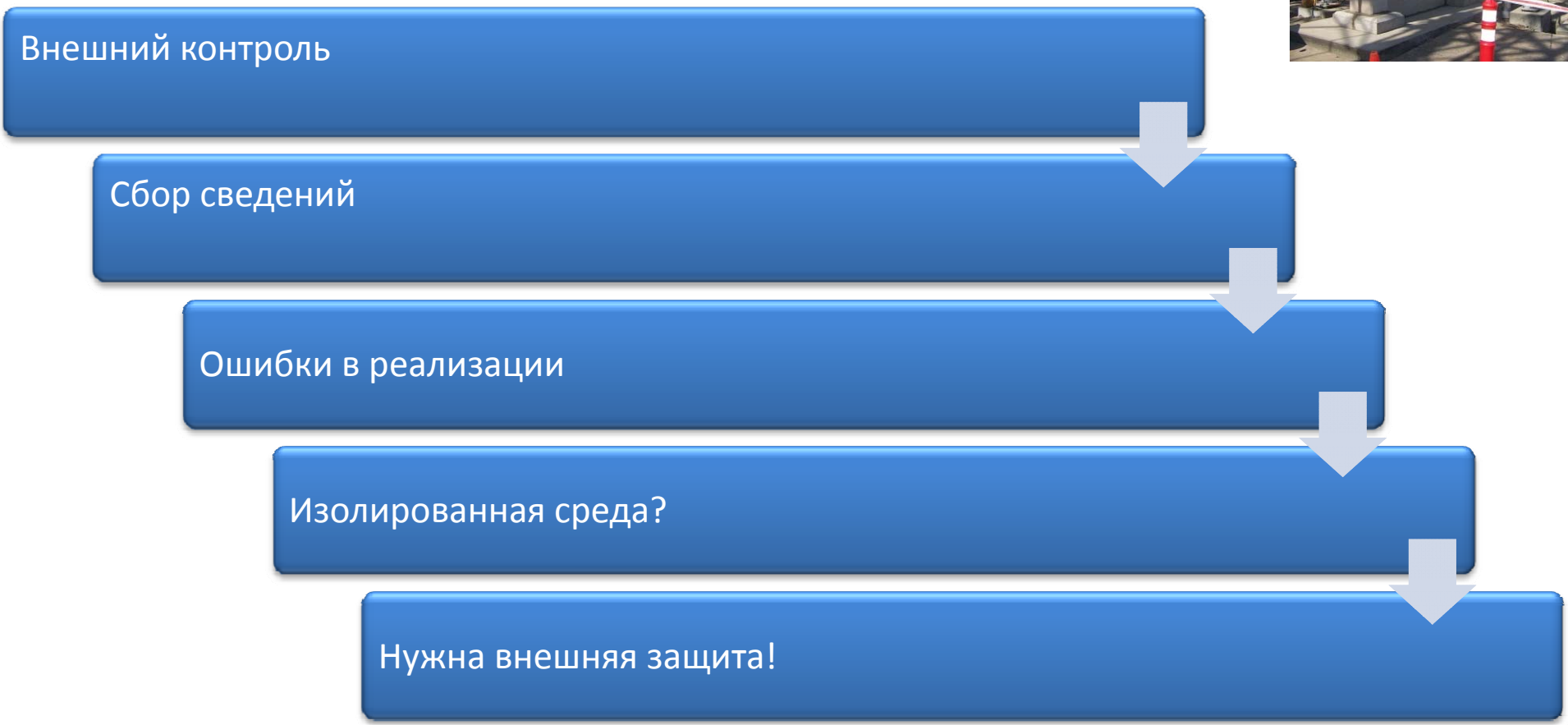
iOS

- НАПРИМЕР, УЯЗВИМОСТЬ В РЕАЛИЗАЦИИ RASCOON (IPSEC IKE) В APPLE IOS

Android

- Исследования NCSU (Woodpecker)

Глубина песочницы



Экосистема



Firewall



iOS

- НЕТ РЕШЕНИЯ В РЕПОЗИТОРИИ ПО

Android

- РЕШЕНИЯ ЕСТЬ,
НО НУЖНЫ ПРАВА СУПЕРПОЛЬЗОВАТЕЛЯ

Песочница



Sandbox+Store+Management

ИЗОЛИРОВАННАЯ СРЕДА?

Или КОММУНАЛЬНАЯ
КВАРТИРА?

Ключ от КОТОРОЙ ВАМ
НЕ ДАЛИ ...



Суперпользователь

БЕЗОПАСНОСТЬ В ПОЛНОМ ОБЪЕМЕ

ВСТРОЕННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ
МОБИЛЬНЫХ ПЛАТФОРМ — ИЛЛЮЗИЯ ДЛЯ
КОРПОРАТИВНОГО СЕКТОРА

Глубокая песочница

Получение контроля над системой

ПРАВА СУПЕРПОЛЬЗОВАТЕЛЯ



Решение вопросов информационной безопасности

ViPNet VPN

Firewall сетевого
уровня

Системное решение

- Политики, мониторинг,
удаленное обновление

Использование
внешних систем ИБ



Sandbox 😊

ViPNet Client

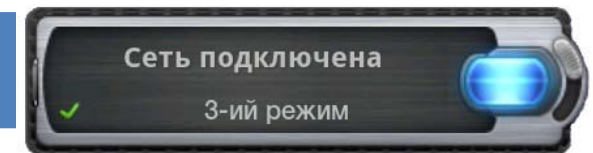
Безопасность

- Защита канала технологиями ViPNet между сетевым и канальными уровнями
- Файервол уровня ОС
- Криптография ГОСТ
- Управление политиками сети ViPNet
- Доступ через корпоративный прокси в соответствии с политиками ИБ



Эргономика

- Эргономичный лаконичный интерфейс
- Поддержка удаленного обновления
- Поддержка Мониторинга
- Оптимизация энергопотребления
- Возможность создания замкнутой среды



ViPNet Client



Рускрипто' 2012



конференция
РусКрипто'2012

СПАСИБО ЗА ВНИМАНИЕ!

Николай Смирнов,
начальник отдела научных исследований и
развития продуктов
дивизиона продаж и партнерских программ
ОАО «ИнфоТекс»



smirnovnv@infotecs.ru



+7 495 737-6192 (доп. 5111)

© 2012, ОАО «ИнфоТекс»

 **infotecs**[®]