НАУЧНО-ИСПЫТАТЕЛЬНЫЙ ИНСТИТУТ СИСТЕМ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ

Построение систем защиты корпоративной инфраструктуры мобильных средств связи на базе систем класса MDM

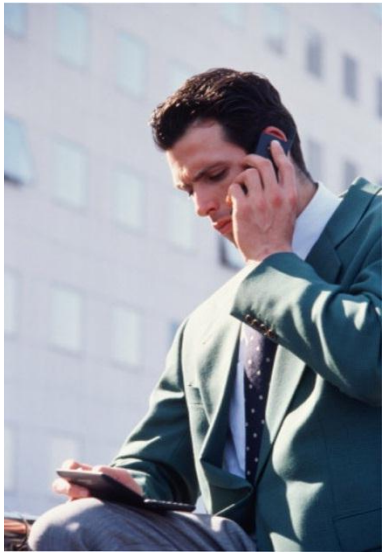
Даниленко Антон,
директор Технического центра
НИИ СОКБ

www.niisokb.ru

Мобильные средства связи (МСС) с точки зрения информационной безопасности

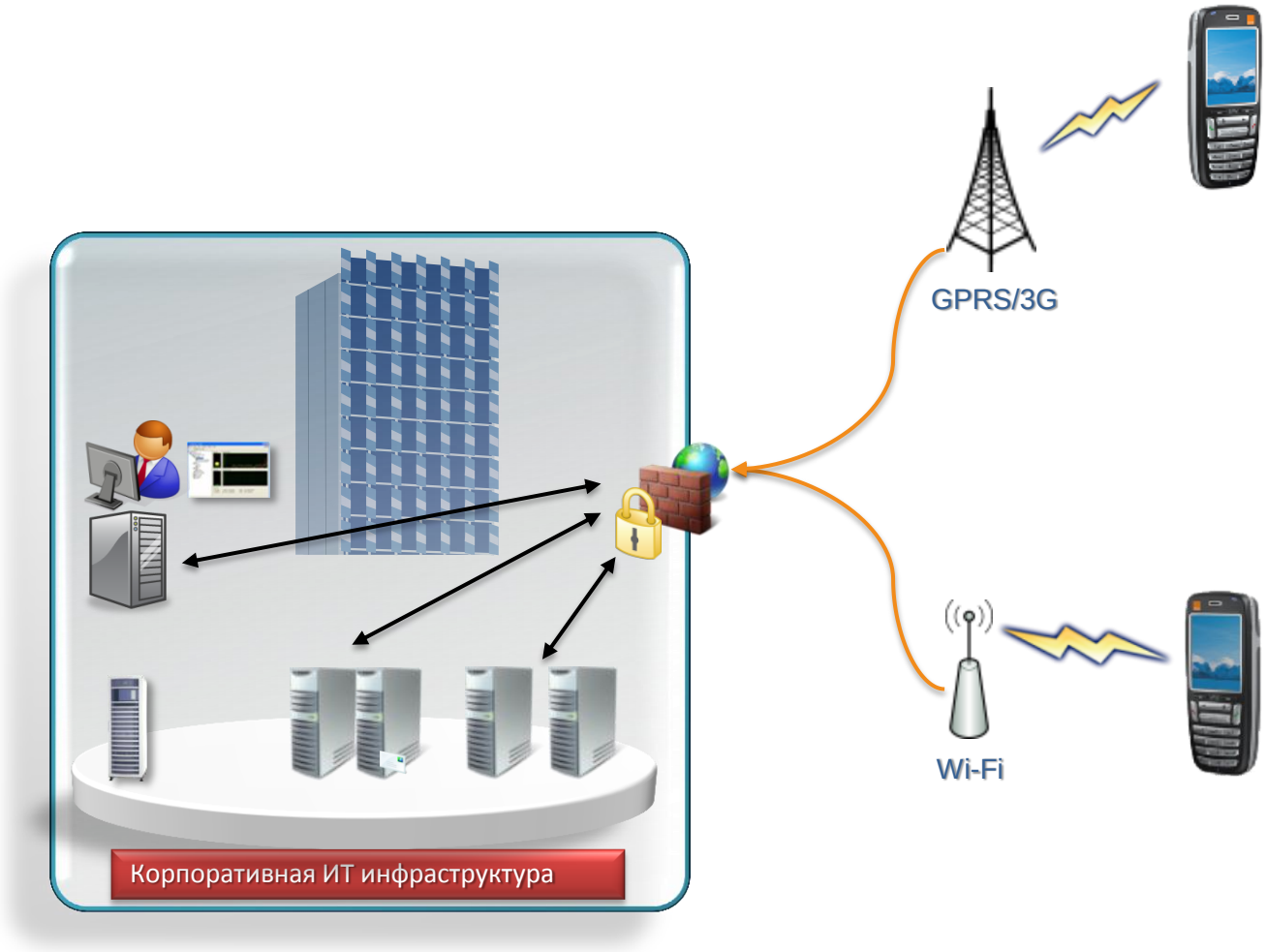
- Хранение информации

- Доступ к информации



- Создание и обработка информации

Мобильные пользователи корпоративной информационной инфраструктуры



Возможности злоумышленника

Доступ в корпоративную сеть

Чтение списка входящих / исходящих вызовов

Чтение данных телефонной книги

Чтение корпоративной почты

Чтение SMS сообщений

Звонки с телефона жертвы

On-line подслушивание (запись) телефонного разговора

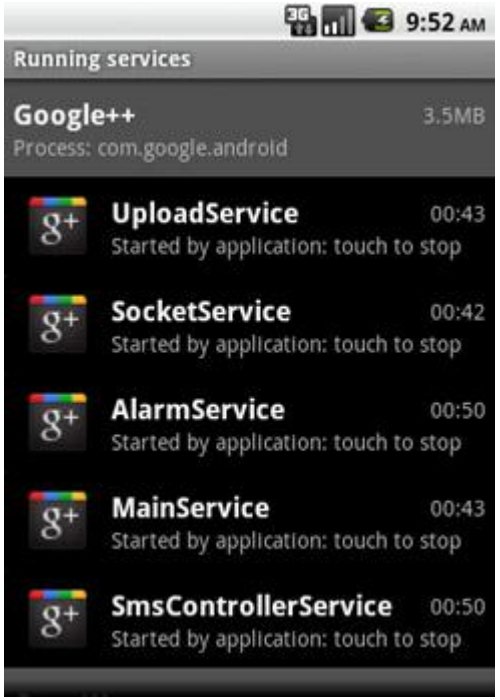
Использование телефона в качестве «жучка» - микрофона

Например

Троян для Android маскируется под приложение Google+

8 Aug 2011

Nickispy.C промышляет чтением текстовых сообщений, журнала вызовов, а также регистрацией местоположения с помощью GPS, передавая эти данные на удаленный сервер. Вредоносная программа способна не только записывать звонки и пересылать аудиофайлы, но и позволяет злоумышленникам прослушивать разговоры в реальном времени



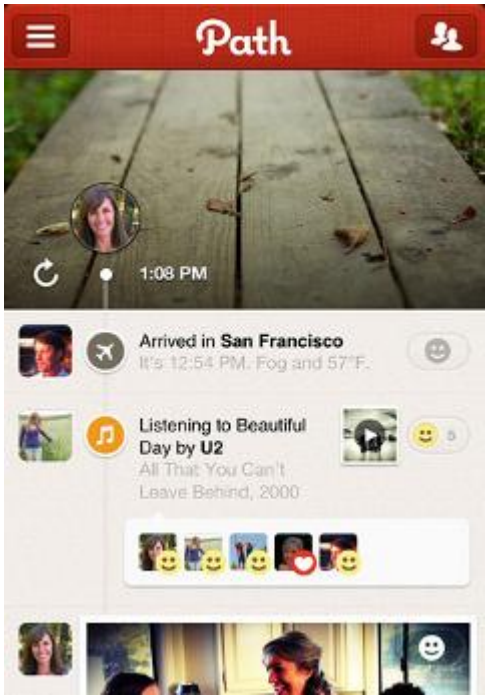
http://www.electronista.com

Например

Соцсеть Path обвинили в "краже" адресных книжек у владельцев iPhone

8 Feb 2012 – Singapore

При каждом запуске программы в руки к разработчикам Path отправляется копия адресной книжки его айфона от A до Z - а именно, данные о всех контактах: имена, фамилии, электронные адреса и телефоны.



Прореху в программе обнаружили совершенно случайно. Если бы эксперт не заинтересовался не полез внутрь клиента, неизвестно, как скоро пользователи узнали бы о ней и узнали ли бы вообще.

http://mclov.in

Варианты установки злонамеренного ПО на мобильное средство связи

Физический доступ к телефону

Взлом по Bluetooth

Взлом по Wi-Fi

Взлом через SMS

Существующие корпоративные решения по управлению и защите МСС

Функциональность	MDM (Microsoft)	RIMEnterpriseServer 5.X(Blackberry)	Good 4.9 (Motorola)	IMS 8.0 (IBM)	Afaria (Sybase)	Symantec Mobile Management	SafePhone
Работа с эл. почтой и мгновенные сообщения	Exchange	X	X	X	One Bridge	X	X
Политики безопасности	X	X	X	X	X	X	X
Интеграция с политиками безопасности домена	X	X	–	–	X	X	X
Запрет на установку ПО на устройствах	X	X	X	X	X	X	X
Запрет интерфейсов устройства (ИК порт, Bluetooth, камера, Wi-Fi)	X	X	–	–	X	X	X
Удаленная рассылка и установка программного обеспечения	X	X	X	X	X	X	X
Удаленное обновление мобильной ОС	–	X	–	–	X	–	–
Удалённое стирание данных на устройстве	X	X	X	X	X	X	X
Мобильная VPN	X	X	–	–	X	X	X
Двухфакторная аутентификация	X	X	–	X	X	X	X
Ведение банка доверенного ПО	–	–	–	–	–	X (IPhone, IPad)	X
Мониторинг передвижения абонентов на карте	–	–	–	–	–	–	X
Просмотр истории SMS/звонков	–	–	–	–	–	–	X
Ограничения на звонки в пределах корпоративной телефонной книги	–	–	–	–	–	–	X
Поддержка МСС основных производителей	–	–	X	X	X	X	X

А также MDM от McAfee, AirWatch и т.д…

Существующие корпоративные решения по управлению МСС

Недостатки некоторых представленных на рынке решений:

• моновендорность некоторых решений (MS MDM, RIM Blackbarry ES)
• отсутствие внедрений на российском рынке – соответственно, отсутствие компетенции
• «тяжеловесность» и перегруженный функционал, высокая стоимость владения
• отсутствие сертификатов государственных регуляторов в области ИБ и возможные проблемы в их получении в будущем

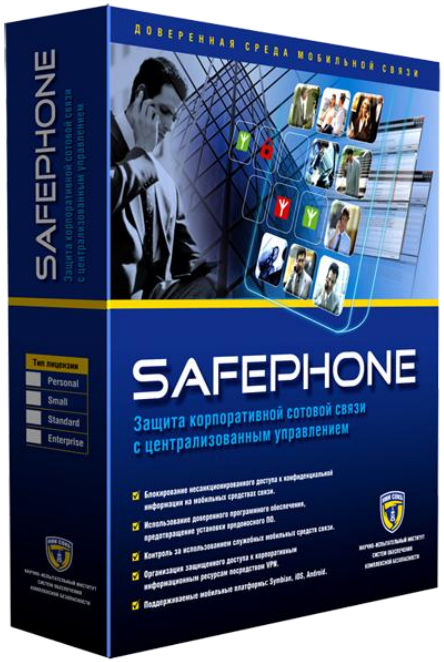
Возможная альтернатива:

Центр управления корпоративной сотовой связью на базе решения от НИИ СОКБ – системы SafePhone

Новое решение на рынке

Центр управления корпоративной сотовой связью на базе решения от НИИ СОКБ – системы SafePhone

SafePhone: назначение решения



- предотвращение несанкционированной установки ПО и, как следствие, предотвращение возможного НСД к конфиденциальной информации
- ведение банка доверенного ПО для установки на МСС
- контроль за использованием МСС в служебных целях
- организация защищённого доступа в корпоративную информационную инфраструктуру посредством VPN

Особенности SafePhone

Безопасность

- неудаляемый с МСС мобильный агент SafePhone
- установка и удаление программ только из банка доверенного ПО
- удалённое блокирование и очистка МСС
- возможность блокирования технических каналов утечки - фотокамеры, диктофона, Bluetooth, Wi-Fi
- доступ в корпоративную инфраструктуру и в Интернет только через шлюз SafePhone
- шифрованый канал связи между МСС и сервером SafePhone
- конфиденциальный обмен сообщениями (внутренняя служба сообщений)

Администрирование

- паспортизация корпоративных МСС
- дистанционная установка политик ИБ на МСС
- дистанционное обновление клиента SafePhone на МСС
- мониторинг приложений
- дистанционное обновление телефонных справочников абонентов
- запрет связи с абонентом, не включённым в справочник
- интеграция со службой каталогов MS Active Directory

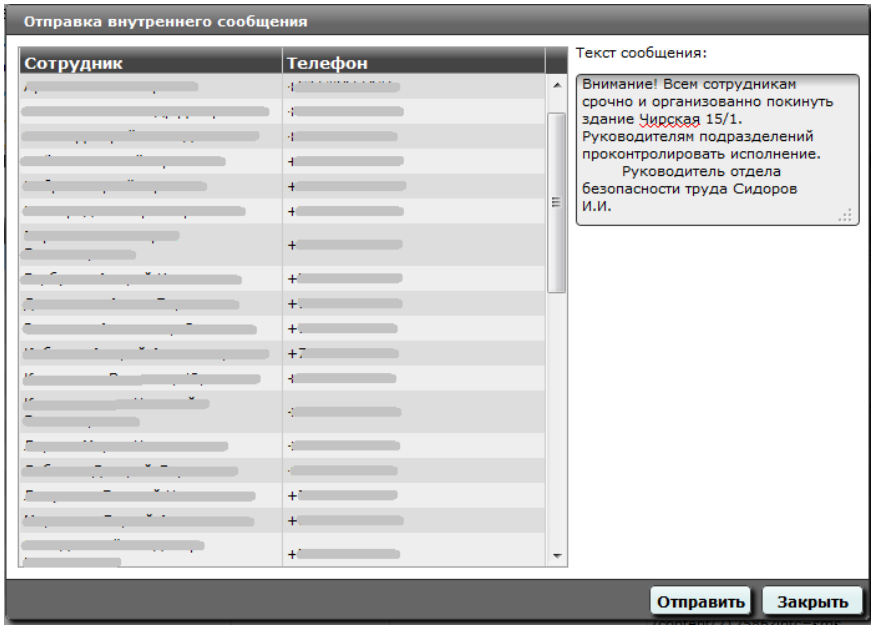
Аудит по МСС

- система построения отчетов по заданным параметрам
- ведение журнала звонков и SMS
- уведомление о смене SIM
- журналирование событий для МСС (состояние аккумулятора, просмотр списка запущенных приложений и т.д.)
- мониторинг времени звонков
- мониторинг передвижения абонентов на карте

Атака на инфраструктуру оператора

SAFEPHONE защита от утечки данных

- обмен внутренними сообщениями без службы SMS
- групповые оповещения без службы SMS



Атака канала сотовой связи

SAFEPHONE защита от перехвата

- шифрование данных, передаваемых между МСС и SafePhone Server
- Возможность исполнения с шифрованием канала российскими криптографическими алгоритмами (ГОСТ)

Атака по Wi-Fi, Bluetooth, …

SAFEPHONE

защита от атак по техническим каналам Wi-Fi, Bluetooth и др.

- управление списком разрешенных точек доступа
- шифрование данных, передаваемых между МСС и SafePhone Server
- блокировка фотокамеры, диктофона

Атака мобильных средств связи

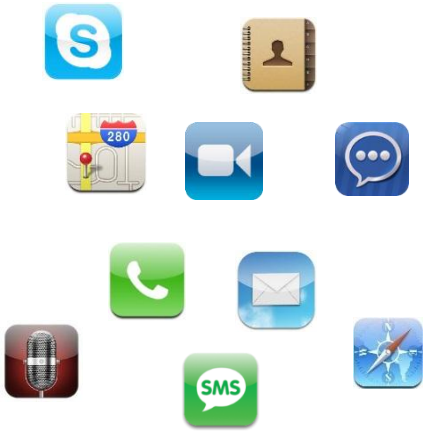
SAFEPHONE защита от физического анализа устройства

- защита от установки любого стороннего ПО
  - ведение банка доверенного ПО для установки на МСС
  - дистанционный контроль инсталляций/деинсталляций программного обеспечения на МСС
- дистанционное блокирование МСС, удаление данных, исключение МСС из системы SafePhone

Атака мобильных средств связи

Скрытная установка агентского ПО

- невидимо для пользователя и антивирусного ПО
- мониторинг и логирование любых событий
- передача любых данных
- аудио-, фото- и видеошпионаж
- удаленное управление МСС



Наиболее эффективная и популярная атака

Атака мобильных средств связи

SAFEPHONE защита от агентского ПО

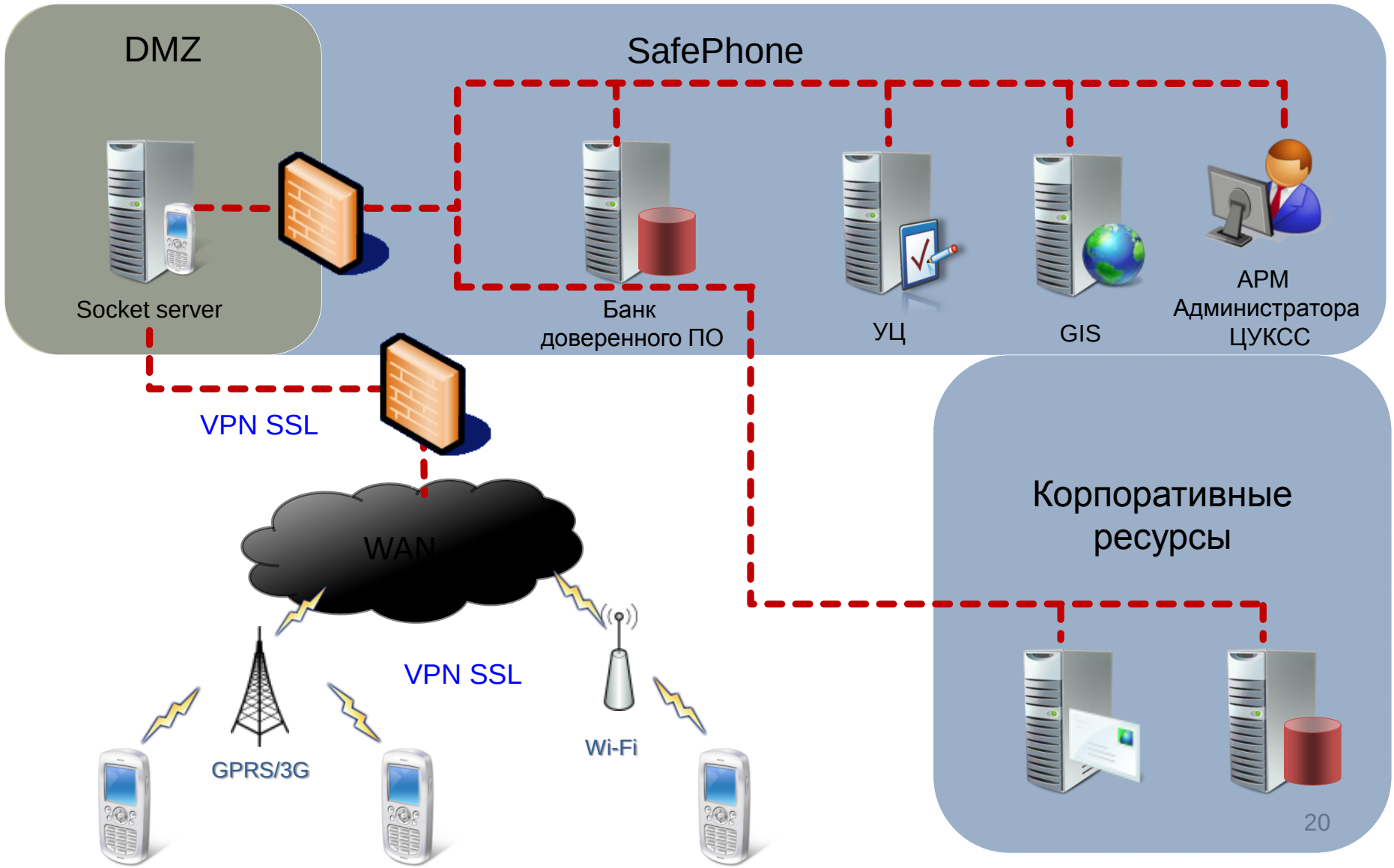
- защита от установки любого стороннего ПО
  - ведение банка доверенного ПО для установки на МСС
  - дистанционный контроль инсталляций/деинсталляций программного обеспечения на МСС
- блокирование интерфейсов (фотокамеры, микрофона, Bluetooth, WiFi)
- корпоративный прокси-сервер с контролем интернет-трафика

Внутренний нарушитель

SAFEPHONE защита от инсайда

- контроль звонков и SMS
- положение на карте
- контроль запущенных приложений на МСС

Архитектура ЦУКСС на базе SafePhone



SafePhone

- Ведение банка доверенного ПО для установки на МСС (установить приложения из других источников невозможно)
- Российская разработка, сертификация у регуляторов (малая вероятность сертификации решений зарубежных конкурентов)
- Возможность «кастомизации» решения под требования заказчика.

СИСТЕМА ДОБРОВОЛЬНОЙ СЕРТИФИКАЦИИ
ГАЗПРОМСЕРТ
РОСС RU.3022.04ГО00

ОРГАН ПО СЕРТИФИКАЦИИ
«Научно–испытательный институт систем обеспечения комплексной безопасности» (ОС «НИИ СОКБ»)
117246, г. Москва, Научный проезд, д. 6, тел. +7(495) 646-75-63, факс +7(495) 646-75-64
№ ГО00.RU.1313 от 15.12.2010

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ ГО00.RU.1313.Н00163 П 1312

Срок действия с 08.02.2012 по 07.02.2015

ПРОДУКЦИЯ
Система защиты корпоративной сотовой связи с централизованным управлением «SafePhone»
«серийный выпуск»

КОД ОКП: 50 0000 (ОК 005) КОД ТН ВЭД РФ:

СООТВЕТСТВУЕТ ТРЕБОВАНИЯМ НОРМАТИВНЫХ ДОКУМЕНТОВ
требованиям по безопасности информации, заданным в технических условиях ТУ 5000-017-95561296-2011

ИЗГОТОВИТЕЛЬ
Закрытое акционерное общество «Национальный Инновационный Центр»
ИНН 7704599880, 119121, г. Москва, Земледельческий переулок, д. 12, тел.: +7(495) 504-16-14, факс: +7(495) 504-16-14, e-mail: info@nic-info.ru

СЕРТИФИКАТ ВЫДАН
Закрытому акционерному обществу «Национальный Инновационный Центр»
ИНН 7704599880, 119121, г. Москва, Земледельческий переулок, д. 12, тел.: +7(495) 504-16-14, факс: +7(495) 504-16-14, e-mail: info@nic-info.ru

НА ОСНОВАНИИ
Протокола сертификационных испытаний от 03.02.2012 № 519-ИЛ-Ф/П ИЛ "ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ" (рег. № ГО00.RU.2216).
Технического заключения от 03.02.2012 № 519-ИЛ-Ф/ТЗ ИЛ "ДОКУМЕНТАЛЬНЫЕ СИСТЕМЫ" (рег. № ГО00.RU.2216).

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ
Сертификация по схеме № 3с

Заместитель Руководителя органа по сертификации — подпись — М.Е. Костенко (инициалы, фамилия)
М.П.
Эксперт — подпись — И.А. Калайда (инициалы, фамилия)

Спасибо за внимание

www.safe-phone.ru

Даниленко Антон,
директор Технического центра
НИИ СОКБ
ADanilenko@niisokb.ru