«SSG Phone»
телефон, защищённый* от прослушивания и перехвата информации

Целевая аудитория: первые лица государств, представители властных структур высшего уровня, спецслужбы, военные, ЧВК, охранные организации, финансисты и юристы.

**Под защищённым телефоном подразумевается смартфон или планшет на платформе Android с уникальной прошивкой. Функции защиты ото всех основных угроз безопасности передачи данных по сетям GSM/UMTS/LTE/Wi-Fi реализовываются при помощи установки авторских операционной системы и программного обеспечения.*

ОПИСАНИЕ

Прошивка (операционная система или ОС) должна быть написана с учётом проверки кода Android на наличие внутренних закладок, позволяющих удалённо управлять любым телефоном в любой точке мира – при помощи скрытых модулей, таких как Galileo (речь о модулях lawful interception, так называемого законного перехвата информации, то есть юридически санкционированного доступа правоохранительных организаций к частным данным устройства в рамках оперативно-розыскных мероприятий). Важна детальная верификация исходного кода профессиональными нативными девелоперами под Android с тесным сотрудничеством с профессионалами в области практической ИТ-безопасности. Все предустановленное стандартное программное обеспечение (ПО), Google Play и проч. в ОС присутствовать не должно.

Операционная система каждый раз должна загружаться со встроенной памяти смартфона в его оперативную память по примеру подобных систем для ПК. Ключевой момент – это полное отсутствие возможности восстановления или извлечения каких бы то ни было данных, использованных системой при сеансе работы, после перезагрузки или выключения устройства. Таким образом защищены списки вызовов, SMS-сообщения, персональный словарь клавиатуры, сообщения электронной почты, история посещения браузера и прочие данные, использованные в том или ином сеансе работы устройства – то есть осуществляется полный запрет записи на внутреннюю память устройства на уровне ОС.

В операционной системе устройства уже будут предустановлены все необходимые программы для безопасной работы. Выход в интернет будет жёстко контролироваться встроенным межсетевым экраном (файрволом) с фильтрами по порту и хосту. Так же возможен предустановленный VPN на защищённый удалённый сервер, при этом выход в сеть осуществляется только при активном подключении через VPN.

Опцию полного выключения устройства необходимо реализовать на уровне «железа» (аппаратный уровень), то есть подразумевается не обычное программное выключение стандартной ОС Android таких функций как камера, модули мобильной связи, Wi-Fi, A-GPS, а также модуль lawful interception, позволяющие осуществление включения телефона с его последующей работой в качестве

микрофона для удалённого прослушивания), а полное выключение устройства, при котором физически невозможны приём и передача каких-либо данных.

Необходимо также реализовать возможности скачивания и инсталляции на пользовательское устройство приложений сторонних разработчиков, при этом включение этих функций на аппаратном уровне стоит защитить сложным администраторским паролем, чтобы обезопасить пользователя от случайных, то есть необдуманных действий.

Если же работы некоторых функций невозможно ограничить при помощи служебной прошивки, их необходимо исключить физически – например модуль A-GPS или камеру можно извлечь из устройства.

При создании телефона необходимо реализовать максимальную защиту, как если бы он использовался в зоне АТО или в любой другой точке с потенциально небезопасной ИТ-инфраструктурой. То есть в случае если у оппонента и получится перехватить данные, у него не будет возможности их расшифровать, равно как и удалённо поразить устройство вирусом или же воспользоваться полученной информацией при физическом захвате смартфона.