Меры безопасности для устройств под управлением Android OS
Гатиятуллин Т. Р.

Гатиятуллин Тимур Радикович/ Gatijatullin Timur Radikovich – студент 4 курса,
Институт управления и безопасности предпринимательства,
Башкирский государственный университет, г. Уфа

Аннотация: *в данной статье рассматриваются проблемы безопасности Android OS и предлагаются меры по защите личных данных.*
Ключевые слова: *информационная безопасность, google, android, вирусы, смартфоны.*

Всем известен тот факт, что Android OS является бесспорным лидером среди операционных систем (ОС) для смартфонов. Так, по итогам минувшего года доля устройств на базе этой ОС составляла более 80 % [1]. Популярность Android-устройств волне объяснима, ведь они отличаются наличием целого ряда преимуществ. К подобным преимуществам можно смело отнести широкое разнообразие доступных моделей, адекватную стоимость и большие возможности персонализации. Тем не менее, внушительное количество людей, использующих данную систему, привлекает внимание злоумышленников.

Открытый исходный код позволяет сменить настройки системы, установить альтернативную версию ОС, и при этом не даёт никаких гарантий безопасности. На примере Android можно видеть подтверждение тому, что чем известнее продукт, тем чаще он подвергается атакам злоумышленников. Первая вредоносная программа на платформе Android была обнаружена в 2010 году, со временем количество вирусных программ значительно увеличилось и до сих пор продолжает расти.

Однако пугаться не стоит, в Android OS встроена защита от вредоносных приложений, и нужно очень постараться, чтобы установить такое приложение на телефон. В Google Play установлены жесткие правила для разработчиков приложений: перед добавлением приложения в магазин, оно проходит тщательную проверку, и шанс установить вирус из магазина Google Play крайне мал. А для установки приложения из неизвестного источника нужно в настройках безопасности системы и снять атрибут «Загрузка только из проверенных источников».

Предположим, что у вас не установлено антивирусное программное обеспечение, и вы являетесь стандартным пользователем смартфона. Каким-то образом вы нашли в Google Play вредоносное приложение и пытаетесь его установить. При попытке установить любое приложение Android OS выводит окно, в котором написано к чему запрашивает доступ устанавливаемое приложение. В этот момент необходимо внимательно прочитать отображаемый список. Если вы устанавливаете приложение для улучшения качества снимков, а оно запрашивает доступ к вашему списку контактов или микрофону, то стоит задуматься, а нужно ли устанавливать такое приложение? Если попытаться установить приложение не из официального магазина приложений Google, то перед установкой необходимо будет в настройках безопасности системы снять атрибут «Загрузка только из проверенных источников», после этого появится указанное выше окно с правами доступа. И даже если после этого вы попытаетесь продолжить установку, появится окно с запросом от Google на разрешение сканирования смартфона для обнаружения подозрительной активности. Эта функция под названием Verify Apps присутствует почти на всех смартфонах под управлением Android. Как мы можем увидеть в Android OS достаточно барьеров защиты против вредоносных приложений, и устанавливать дополнительно антивирус не совсем разумно, ведь данное приложение постоянно работает в фоновом режиме, сканирует все приложения, следит за веб-трафиком, выводит надоедливые уведомления и тратит на это ресурсы смартфона, сокращая длительность работы от аккумулятора [2].

Достаточно соблюдать несколько разумных правил, позволяющих не устанавливать антивирус. А именно: не менять настройки безопасности, установленные по умолчанию; не устанавливать приложения из неизвестных источников или с плохой репутацией в магазине приложений. Если вы беспокоитесь о приватности - проверяйте, не требуют ли приложения доступа к сообщениям, контактам или местоположению. Использовать пароль для блокировки дисплея. Также можно зашифровать все личные данные, хранимые на устройстве, для этого нужно зайти настройки, потом найти вкладку безопасность, а там выбрать пункт «зашифровать устройства» и тогда вся важная информация на смартфоне будет зашифрована. Если вы боитесь, что ваши поисковые запросы кто-то сможет отследить, следует использовать VPN (виртуальную частную сеть), обеспечивающую приватность при пользовании Интернетом. Для безопасного общения в сети, используйте специализированные для этого приложение, например Telegram или Chatsecure. Также не нужно постоянно использовать службы геолокации, лучше удалять ненужные программы, и желательно собирать сведения о новых приложениях перед их установкой [3]. Данные меры обезопасят ваш смартфон от большинства угроз.

Литература

1. Борис Владимирович. Google Android — становится стандартом де-факто для мобильных устройств [Электронный ресурс]: Geektimes. Режим доступа: http://geektimes.ru/post/248122/ (дата обращения: 05.01.2016).
2. Вячеслав Голованов. Почему антивирусы под Android бесполезны, и что с этим делать [Электронный

ресурс]: Geektimes. Режим доступа: http://geektimes.ru/post/249824/ (дата обращения: 04.01.2016).
3. Как улучшить защиту персональных данных на Android-устройствах? [Электронный ресурс]: anTidroid. Режим доступа: http://antidroid.net/kak-uluchshit-zashhitu-personalnyx-dannyx-na-android-ustrojstvax.html (дата обращения: 06.01.2016).