Д. Колисниченко

БЕЗОПАСНЫЙ ANDROID: ЗАЩИЩАЕМ СВОИ ДЕНЬГИ И ДАННЫЕ ОТ КРАЖИ

- Шифрование данных, хранящихся на Android-устройстве
- Шифрование передаваемых данных
- VPN-соединения
- Анонимизация трафика с помощью Tor
- Ограничение запуска приложений
- Антивирусы и брандмауэры
- Поиск потерянного или украденного устройства
- Вопросы семейной безопасности
- Экономия трафика, защита от спама
- Получение прав root

bhv

УДК 004.4
ББК 32.973.26-018.2
К60

Колисниченко Д. Н.

К60 Безопасный Android: защищаем свои деньги и данные от кражи. — СПб.: БХВ-Петербург, 2015. — 161 с.: ил.

ISBN 978-5-9775-3149-8

Рассмотрены различные способы обеспечения безопасности Android-устройств: шифрование персональной информации, хранящейся на устройстве, шифрование передаваемых данных, VPN-соединения, анонимизация трафика, выбор и использование антивируса и брандмауэра, поиск потерянного или украденного устройства, экономия трафика, защита от спама, получение прав root. Уделено внимание вопросам личной и семейной безопасности (ограничение доступа ребенка к определенным ресурсам/программам, отслеживание телефона ребенка и т. д.). Практически все рассмотренное в книге программное обеспечение бесплатное, что поможет не только защитить ваше устройство, но и сэкономить деньги.

Для широкого круга пользователей Android

УДК 004.4
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Екатерина Капалыгина*
Редактор	*Григорий Добин*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн обложки	*Марины Дамбиевой*

Подписано в печать 30.01.15.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 12,9.
Тираж 1500 экз. Заказ №
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Первая Академическая типография "Наука"
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-3149-8

Оглавление

ГЛАВА 1

Как не превратить свой смартфон в «кирпич»?

1.1. Немного об эволюции мобильного телефона

Современный мобильный телефон уже давно превратился в небольшой персональный компьютер с полноценной операционной системой. Еще десять лет назад сломать мобильный телефон можно было лишь физически: разбить, утопить или совершить прочие подобные акты вандализма по отношению к довольно-таки полезному устройству. За эти десять лет многое изменилось, поменялось даже название самого мобильного телефона — теперь их называют *смартфонами*, чтобы подчеркнуть, что это не просто мобильный телефон, а устройство с дополнительными «умными» (smart) функциями.

Итак, во-первых, *унифицировано системное программное обеспечение*. Да, десять лет назад на мобильные устройства также можно было устанавливать приложения. Речь здесь, конечно, не идет о совсем уж «древних» аппаратах конца 1990-х — начала 2000-х годов. Эти динозавры нужно было «перепрошивать» даже для простого изменения мелодии, не говоря уже об установке программ. Но на более «современные» телефоны прошлого десятилетия уже можно было устанавливать дополнительное программное обеспечение. Однако и здесь не все было так просто — программное обеспечение разных производителей, как правило, оказывалось не совместимым между собой. Например, вы не могли скачать программу для Siemens и установить ее на Nokia. Более того, несовместимым часто могло быть программное обеспечение, написанное для разных моделей одного и того же производителя. Такая ситуация напрочь отбивала желание вообще что-либо устанавливать. Даже если какую-нибудь программу (а их было не так уж и много) и удавалось установить, то это событие отмечалось как маленькая победа.

Но вот, в 2008 году, свершилось чудо — была разработана ОС Android. Эта операционная система обеспечила столь необходимую универсальность, и теперь вы можете устанавливать (и удалять) Android-программы на любой смартфон, работающий под управлением Android, хоть по нескольку раз на дню: установил — не понравилось — удалил. Никаких ограничений нет (если не считать того, что неко-

торые приложения — коммерческие). Казалось бы, вот оно счастье! Но не тут-то было. Свобода несет в себе и некую опасность. Пользователь, например, может установить вредоносную программу, замаскированную под необходимый для него программный продукт. Взять тот же навигатор Navitel — это коммерческая программа, и пользователь может использовать ее бесплатно лишь 30 дней, после чего нужно купить ключ. Некоторым несознательным пользователям покупать ничего не хочется, поэтому они устанавливают Navitel из непроверенного источника и вместе с навигатором получают «троянского коня». Что будет делать этот «конь», зависит только от фантазии его разработчиков. Он может, например, обеспечивая функционирование навигации (т. е. Navitel все-таки будет в комплекте), записывать и пересылать третьей стороне все телефонные разговоры, SMS, фотографии и другие ваши конфиденциальные данные. А может просто взять и удалить все пользовательские данные с карты памяти устройства. Особо «злые» программы могут даже уничтожить ваш смартфон, превратив его в «кирпич».

Во-вторых, *изменилась функциональность устройства*. Теперь оно «напичкано» всевозможными датчиками. Если раньше телефон имел только динамик, микрофон и, может быть, веб-камеру весьма сомнительного качества, то сейчас не хватает, наверное, лишь датчика дождя. Все остальное в ваш смартфон уже встроено. К счастью, наличие этих датчиков (сенсоров) никак не может повредить непосредственно устройство, но представляет собой в некотором роде проблему для самого его владельца. Так, ориентируясь на GPS-модуль устройства, можно отследить его перемещение на местности. Конечно, оператор мобильной сети и так может следить за перемещениями пользователя, даже если у него обычный телефон десятилетней давности. Но здесь речь идет о том, что любой желающий, завладевший вашим телефоном всего на несколько минут (например, когда вы в офисе забыли его на столе, или просто попросивший его у вас, чтобы якобы поговорить по телефону, поскольку его собственный телефон разрядился), может установить некое приложение, которое будет следить за всеми вашими перемещениями и сообщать о них, куда надо. Согласитесь, это не очень хорошо. Точно так же существуют приложения, которые постоянно или по команде извне могут начать запись и трансляцию в нужном направлении всего, что происходит в данный момент вокруг устройства — т. е. ваш смартфон будет использоваться как обычный «жучок». И поверьте, не нужно быть семи пядей во лбу, чтобы разработать такие приложения.

В-третьих, теперь, кроме списка SMS, адресной книги и перечня последних набранных номеров, *в смартфоне хранится серьезная личная информация*. Возможности Android позволяют устанавливать на смартфоны и планшеты обычные офисные приложения, а это означает, что в памяти вашего мобильного устройства могут содержаться важные документы, конфиденциальная переписка по электронной почте, личные фотографии и прочие данные, которые могут использовать против вас конкуренты или «доброжелатели». Всю такую информацию нужно защищать. И сегодня это не проблема, поскольку на современных смартфонах установлены мощные многоядерные процессоры, для которых шифрование — по зубам. В *главе 4* мы как раз и рассмотрим способы защиты ваших персональных данных. Но если этот вопрос беспокоит вас больше прочих, вы можете перейти к ее чтению прямо сейчас, а затем уже дочитать пропущенные главы.

1.2. Меры предосторожности

Теперь поговорим о том, как не испортить ваш ~~мобильный телефон~~, ой, смартфон. Начнем с мер физической предосторожности. Все-таки смартфон — сложное и относительно дорогое устройство, и хочется, чтобы оно работало долго и безотказно. Все мы люди адекватные и прекрасно понимаем, что бросать смартфон об стену, пытаться утопить его или бить по нему молотком — не сто́ит. Конечно, существуют специальные защищенные модели, выпускаемые компаниями Sigma и Tetex, они предназначены для экстремального использования, однако большинство устройств не выдержит и половины того, что могут выдержать защищенные аппараты.

Вот несколько советов, следование которым позволит сохранить смартфон или планшет в целости и сохранности хотя бы физически:

- **купите защитный чехол** — он не только убережет устройство от царапин, но и существенно повысит шансы его выживания при падении. Чехол также удобен и тем, что при падении смартфон не рассыплется на несколько частей: заднюю крышку, аккумулятор и т. п.;
- **старайтесь не говорить под дождем** — полагаю, не нужно рассказывать, почему влага это плохо. Опять-таки, от небольшого дождя спасет чехол;
- **остерегайтесь перепада температур**. Одним не очень прекрасным утром я обнаружил, что сенсорный дисплей моего смартфона не работает, хотя вечером все было прекрасно. Вердикт сервисной службы гласил — попала влага. И поскольку под дождь я с ним не попадал и под краном его не мыл, видимо, виной всему оказался конденсат. Отделался я легким испугом — смартфон полежал в разобранном состоянии несколько дней, а когда его собрали, то он заработал, хотя изначально предлагалось поменять сенсорный экран — хорошо что в сервисе его не было в наличии, а доставка затянулась.

  Итак, когда вы выходите из теплого помещения на мороз, не нужно сразу вытаскивать смартфон, пусть он полежит с полчаса в кармане и постепенно остынет. Карман сыграет роль «термоса». Аналогично, когда вы заходите с мороза в теплое помещение, не следует без крайней необходимости пользоваться смартфоном — пусть он те же полчаса полежит в кармане или сумке. По себе знаю, придерживаться этого совета очень сложно, но мое дело рассказать, а ваше — сделать выводы... и продолжать использовать смартфон как обычно;
- **у планшета должен быть свой «дом»** — найдите место, например, на столе возле ноутбука, где планшет должен находиться всегда, когда вы его не используете. Если бросать планшет где угодно, на него элементарно можно сесть, наступить и т. п. То же самое касается и смартфона, хотя придерживаться этого правила весьма трудно. Пишу эти строки, а сам пытаюсь вспомнить, где же мой смартфон...

Физические меры предосторожности — это хорошо, но чаще смартфоны и планшеты приходят в негодность не из-за физического воздействия, а вследствие неправильных действий пользователя. Если вы внимательно прочитали первый раздел

этой главы, то понимаете, что к выбору программного обеспечения нужно относиться очень и очень серьезно. Вот еще несколько полезных правил:

- **никогда не устанавливайте приложения из непроверенных источников**, даже если назначение их вам понятно. Такие приложения могут содержать вредоносный код, который способен сделать с вашим устройством все, что ему заблагорассудится. В идеале рекомендуется устанавливать приложения только из официального магазина приложений Google Play Маркет. Во-первых, все приложения, размещаемые в Play Маркет, проходят проверку, и вероятность наличия в них вредоносного кода — практически нулевая. Во-вторых, там вы можете ознакомиться с рейтингом приложения и отзывами пользователей. Учитывая многомиллионную аудиторию Google Play Маркет, его рейтинг можно считать объективным;
- **не устанавливайте приложения, особенно системные, назначение которых вам непонятно**. Если вы не знаете, что делает программа, лучше ее не устанавливать даже из любопытства;
- **не посещайте сомнительные сайты** со своего планшета или смартфона. Знайте, что «привести в чувство» обычный компьютер, как правило, проще, чем смартфон или планшет. Да и антивирусы для обычных компьютеров более совершенные;
- некоторые приложения (особенно тесно интегрирующиеся с самой системой) требуют прав пользователя root. Сама по себе **процедура получения прав root — опасна**. Если вы не уверены, что вам это нужно, лучше даже не начинать. В *главе 10* мы рассмотрим способы получения прав root для некоторых смартфонов, однако, если существует возможность установить альтернативное приложение, которому для работы не нужны права root, лучше установить именно его. К тому же, активировав права root, вы автоматически лишаетесь гарантии на устройство из-за вмешательства в его микропрограммное обеспечение;
- если вы сомневаетесь в своих силах, умениях и навыках, **лучше забыть о «перепрошивке» устройства**, т. е. об установке новой версии Android. Такую операцию следует производить в сервисном центре, где опыта у специалистов побольше, чем у вас. После неудачной прошивки, а также после неудачной попытки получения прав root может статься, что вам не помогут даже в сервисном центре.

В целом, все достаточно просто — соблюдая изложенные здесь правила, вы существенно продлите жизнь своему устройству.

ГЛАВА 2

Общая безопасность Android-устройства

В предыдущей главе мы поговорили о том, чего *не следует делать*, чтобы не превратить свое дорогое и современное устройство в никому не нужный «кирпич». Здесь же мы посмотрим на проблему с другой стороны, а именно — поговорим о том, что *нужно делать*, чтобы обезопасить свои данные, свое устройство и себя.

Далее приведено несколько простых рекомендаций. Позже, в последующих главах, каждая из рекомендаций будет рассмотрена подробно.

2.1. Отказ от установки приложений из неизвестных источников

Очень часто причиной всех несчастий для владельцев Android-устройства является установка вредоносной программы. Чтобы исключить хотя бы неявную или случайную установку такой программы, рекомендуется запретить установку программ из неизвестных источников.

Безопасным источником считается только Google Play Маркет — по сути, так оно и есть. В этом смысле, например, ваша SD-карта — тоже неизвестный источник, поэтому просто так установить APK-файл, присланный приятелем, уже не получится. Зато вы предотвратите потенциальную угрозу.

Для отключения установки из неизвестных источников перейдите в меню **Настройки | Безопасность** и *выключите* (снимите соответствующую птичку) параметр **Неизвестные источники** (рис. 2.1).

Чтобы вновь получить возможность устанавливать APK-файлы, полученные извне, включите этот параметр для конкретной установки. По крайней мере, вы установите данные APK-файлы осознанно. Думаю, не стоит говорить, что для большей безопасности после установки требуемых APK-файлов параметр **Неизвестные источники** следует выключить снова.

Рекомендуется также включить параметр **Проверять приложения** — система тогда будет блокировать запуск потенциально опасных приложений. Жаль, что этот параметр появился в Android, только начиная с версии 4.1, и его не было в предыдущих версиях.

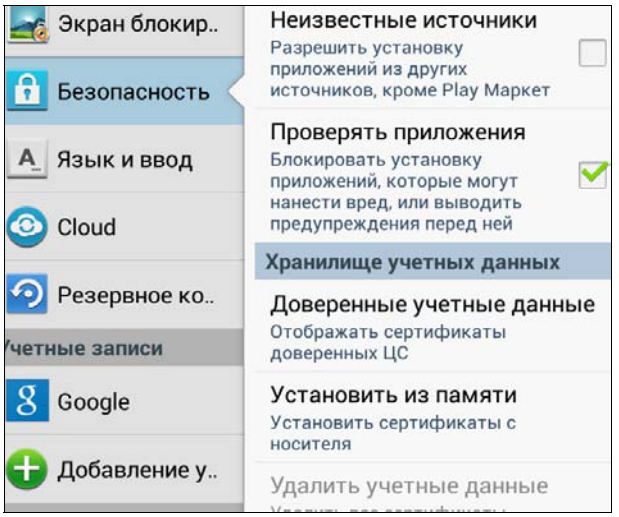

Рис. 2.1. Отключение установки из неизвестных источников

2.2. Осторожно: неизвестные сети Wi-Fi!

Не подключайтесь к неизвестным сетям Wi-Fi, особенно к публичным, происхождение которых вам неизвестно. Может быть, кто-то просто не смог правильно настроить маршрутизатор Wi-Fi, не установил на нем соответствующий пароль, и теперь к его сети может получить доступ любой желающий, и вы в том числе. А может, такая сеть развернута злоумышленниками преднамеренно, чтобы перехватывать все передающиеся по ней данные, в том числе и конфиденциальные, такие как пароли и номера кредитных карточек, и сопутствующую финансовую информацию.

Вообще, с осторожностью относитесь к публичным сетям (аэропорта, ресторана, отеля и т. п.). Никогда нельзя знать, как они настроены. Если приходится передавать данные по таким сетям, шифруйте передаваемые данные. О защите передаваемых по сети данных мы поговорим в *главе 6*. Из нее вы также узнаете, как скрыть свой IP-адрес и получить хоть какую-то анонимность.

Способы шифрования передаваемых данных

Забегая вперед, отмечу, что существуют два способа шифрования передаваемых данных, доступных в Android. Первый заключается в организации VPN-соединения (от англ. ***V**irtual **P**rivate **N**etwork* — виртуальная частная сеть), второй — в использовании Tor (от англ. ***T**he **O**nion **R**outer* — системы так называемой «луковой маршрутизации», создающей каскад из прокси-серверов, что позволяет устанавливать анонимное сетевое соединение, защищенное от прослушивания). Первый способ удобнее тем, что будет зашифрован весь интернет-трафик всех приложений. Но VPN-сервисы обычно платные, т. е. за VPN-трафик придется заплатить. Впрочем, некоторые сервисы предоставляют 100–150 Мбайт бесплатного трафика, чтобы вы могли протестировать скорость и надежность VPN-соединения, чем иногда удается воспользоваться. А вот система Tor бесплатна полностью, вот только не всегда скорость работы через нее соответствует вашим ожиданиям. Кроме того, если вы не получили на своем смарт-

фоне права root (см. об этом в *главе 10*), то через Tor будут работать не все приложения, а только те, которые поддерживают Orbot (официальную версию Tor-клиента для Android). Надеюсь, я вас заинтересовал, и теперь вы не пропустите *главу 6* ☺.

2.3. Установка антивируса

Чтобы обеспечить безопасность самого устройства, установите антивирус. К сожалению, Android тоже может «подхватывать» вирусы. Конечно, «вирусы для Android» — это громко сказано, и в таком понимании, в котором они существуют для Windows, в Android их нет хотя бы потому, что в 99 процентах случаев пользователю не предоставлены root-права, и вирус даже при всем своем желании не может натворить ничего такого, что могло бы причинить вред самой Android. А оставшийся один процент — это пользователи, которые сами получили root-доступ. Пусть теперь пеняют на себя.

В мире Android вирусы — это программы-нарушители, но от этого не легче. Например, такая программа может подслушать вас, отправить SMS на платный номер, украсть ваши личные данные — например, Google-аккаунт или приватные фотографии и т. п. К тому же, вы можете обмениваться файлами, например, документами MS Office, содержащими вирусы. Вот все такие попытки и должен пресечь Android-антивирус.

Самой Android такие вирусы, скорее всего, не навредят, но инфицированные файлы, переданные вами на Windows-компьютеры, могут там причинить вред. О выборе антивируса мы поговорим в *главе 5*. Из нее вы узнаете, какой антивирус лучше, а также ознакомитесь с общими рекомендациями, позволяющими исключить вероятность заражения смартфона.

2.4. Включение шифрования и использование других средств защиты данных

Для защиты личных данных — например, важных документов, фотографий — одного графического пароля или пинкода мало. Если ваше устройство (смартфон, планшет) попадет в руки злоумышленников, то знайте — избавиться от графического пароля очень просто (см. об этом в *главе 10*). Да проще простого извлечь из смартфона карту памяти и прочитать ее на другом устройстве (например, на ноутбуке). Поэтому важные данные можно и нужно шифровать. Шифрованию данных посвящена *глава 4* этой книги.

Для защиты личных данных можно использовать и другие средства — например, программы, скрывающие папки и запрещающие запуск определенных приложений. Может быть, толку от них и не много, но эти средства все же лучше, чем ничего. В частности, они помогут скрыть важные данные от любопытных коллег, когда вы забудете телефон на столе и ненадолго отойдете.

Android-устройство можно в некоторой степени использовать и для обеспечения собственной безопасности. Например, с помощью специальных программ превратить смартфон в «тревожную кнопку», в небольшую систему видеонаблюдения и в диктофон, позволяющий записывать не только происходящее вокруг, но и ваши телефонные разговоры. Все эти вопросы будут рассмотрены в *главе 9*.

2.5. Отключение GPS-модуля

Во избежание отслеживания вашего передвижения (некоторые вредоносные программы могут передавать ваши GPS-координаты третьей стороне) отключите GPS-модуль, когда вы ним не пользуетесь. Конечно, есть и моменты, когда GPS необходим. В этом случае придется определить, какая программа (кроме программы навигации) обращается к демону `gpsd`.

Отключение GPS-модуля также поможет сэкономить заряд аккумулятора. Именно поэтому я рекомендую всегда отключать GPS, когда он вам не нужен. Лично мой планшет с включенным GPS-модулем значительно быстрее разряжается (а при запущенной программе навигации его вообще хватает на 3 часа).

Для отключения GPS и вообще функции определения вашего местоположения перейдите в меню **Настройки | Местоположение** и выключите параметры **Использовать GPS**, **Беспроводные сети** и **Доступ к данным о моем местоположении** (на рис. 2.2 все эти параметры как раз включены).

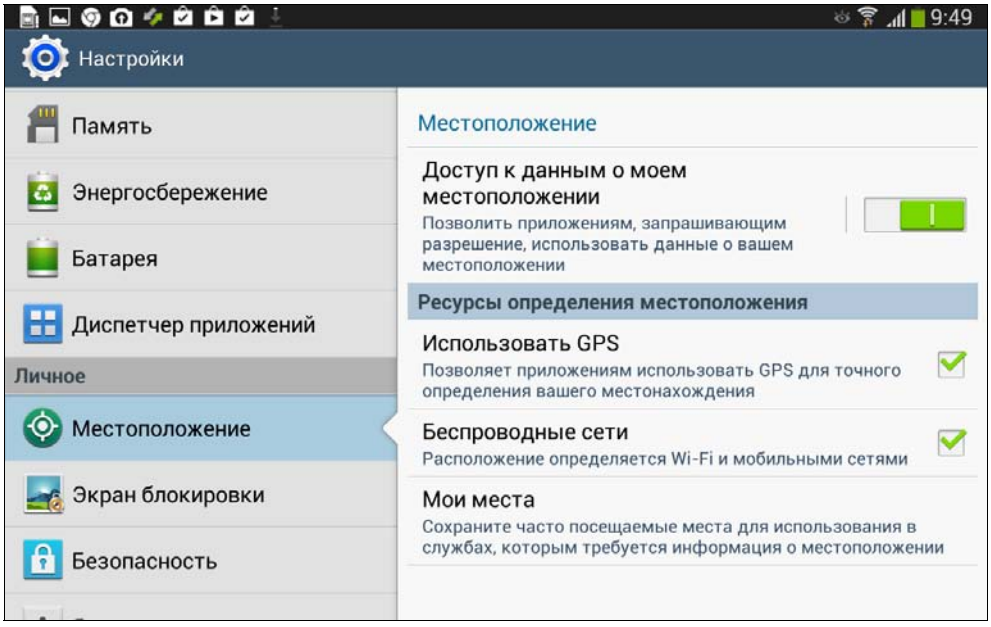

Рис. 2.2. Отключение определения местоположения

Помните, что отключение этих параметров всего лишь не позволит программам получать доступ к данным о вашем местоположении. Если вы не хотите, чтобы оператор сети знал[1], где вы находитесь, выключите устройство и извлеките из него аккумулятор. Кнопка выключения — это не аппаратное выключение, когда физически размыкаются контакты, а всего лишь так называемый *soft-off* — т. е. теоретически устройство все еще может принимать и передавать данные. Гарантировать, что произошло полное отключение устройства может лишь извлечение аккумулятора. При этом аккумулятор легко извлекается из большинства смартфонов, однако аккумуляторы планшетов в большинстве случаев извлечь нельзя, к сожалению.

[1] Может ли оператор установить местоположение выключенного телефона? Ответ на этот вопрос читайте по адресу: **http://habrahabr.ru/post/112449/**.

ГЛАВА 3

Как избавиться от повышенного расхода трафика?

3.1. Куда девается трафик?

Начнем эту главу с рассмотрения весьма беспокоящего момента — расхода трафика. До знакомства с Android я не мог ответить на два вопроса: откуда берется пыль и куда деваются деньги? Сейчас к списку интересующих меня вопросов добавился еще один: куда девается трафик?

Перерасход трафика особенно заметен пользователям, которые перешли на Android с устройств с системами Bada и Symbian на борту. Конечно, самый удобный способ забыть об этой проблеме — купить пакет с безлимитным Интернетом. Однако это не всегда имеет смысл, поскольку у так называемых «безлимитных» пакетов нередко не совсем приличные тарифы на обычные телефонные звонки. Поэтому особой выгоды добиться так не получится: если Интернет будет дешевым, а обычные звонки — нет. Купить еще одну SIM-карту и использовать ее, когда нужно работать в Интернете, — тоже не всегда выход, т. к. в этом случае вы не сможете воспользоваться интернет-виджетами (тем же прогнозом погоды) — т. е. включить-то их будет можно, но на обычной SIM-карте интернет-тариф вам не понравится.

3.2. Аппаратное решение

Для разрешения ситуации можно предложить сугубо аппаратное решение. Все смартфоны умеют подключаться к Интернету по Wi-Fi, поэтому достаточно купить мобильный маршрутизатор (роутер) Wi-Fi, установить в него SIM-карту с самым дешевым доступом к Интернету и получить Интернет на смартфон от роутера по Wi-Fi (при этом совсем не обязательно, чтобы оператор этой сети совпадал с вашим основным). Получается, что в вашем смартфоне стоит SIM-карта оператора, тарифы на телефонные звонки которого вас устраивают больше всего, а в маршрутизаторе установлена SIM-карта оператора, у которого самый дешевый Интернет.

Мобильный маршрутизатор Wi-Fi — весьма компактное устройство. Все мы знаем, как выглядят обычные домашние или офисные маршрутизаторы. Хотя их размеры уменьшаются с каждой новой моделью, все равно они достаточно большие, и но-