ЛЕКЦИЯ 1 - ОСНОВНЫЕ МЕТОДЫ И СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СМАРТФОНАХ

ВВЕДЕНИЕ

Современные технологии позволяют мобильным устройствам потягаться функционалом с настольными компьютерами и ноутбуками. Смартфоны предлагают много новых способов для связи между людьми, для получения, передачи и распространения информации. Это больше, чем сотовая связь. Смартфон умеет подключаться к интернету не только через оператора сотовой связи, но и по wi-fi (как ноутбук в интернет-кафе).

Конечно, смартфон по-прежнему позволяет делать обычные звонки. Но логичнее рассматривать эти устройства как маленькие компьютеры. Функционал смартфона впечатляет. Веб-браузер, электронная почта, голосовая связь, обмен мгновенными текстовыми сообщениями через интернет. Запись, хранение и передача аудиоматериалов, видео и фотографий. Социальные сети, многопользовательские игры, банковские операции и многое другое. Однако новые возможности открывают дорогу новым угрозам безопасности – или усложняют существующие проблемы.

К примеру, в современных смартфонах есть функции GPS. Смартфон и без GPS может выдавать оператору сотовой связи ваше точное местоположение. Не только оператору, но и другим приложениям в смартфоне (например, программам для работы с социальными сетями, картами, веб-сайтами). И если обычный мобильный телефон позволяет оператору сотовой связи приблизительно узнать ваше местоположение, то GPS повышает точность и к тому же расширяет список "адресатов", которым передаются данные.

1.1. ЦЕННОСТЬ ИНФОРМАЦИИ В СМАРТФОНЕ

Человеку обычно хватает интуиции, чтобы не расстаться с бумажником. Каждый знает, сколько там ценного в нем, помимо денег. Потерять бумажник – значит поставить под угрозу свою частную жизнь и безопасность. То же касается смартфона. Потерять смартфон не только жалко и обидно – это еще и рискованно. Смартфон – маленький компьютер, к тому же постоянно подключенный к сети. Есть заметная разница между таким "активным" (и даже интерактивным) устройством и "пассивным" бумажником.

Простой пример. Человек берет свой бумажник и вытряхивает из него содержимое. Что он видит?

- Две фотографии родных и близких.
- Водительские права.
- Две банковские карточки.
- Пять клубных и дисконтных карточек (магазины, автозаправки и т.д.).
- Страховой полис.
- Несколько документов – справки, чеки.
- Деньги (10-15 купюр).

А что в смартфоне?

- Телефонная книжка: 200 рабочих контактов, номеров друзей и близких, некоторые с адресами, днями рождения и прочей информацией.
- История телефонных звонков.
- История отправленных и полученных СМС.
- Фотографии родных, близких, детей, коллег, друзей, снимки из различных поездок (150 штук).
- Видеозаписи (10 штук).

- Сообщения электронной почты (100 штук).
- Настроенные приложения для электронной почты, социальных сетей, других онлайновых служб (5 пар логин-пароль).
- Банковские данные (например, пин-коды карточек, чтобы не забыть).
- Настройки доступа к домашней сети wi-fi (с паролем, естественно).
- Важные заметки, сделанные в пути (30 штук).
- Календарь с планируемыми встречами.

Чем больше вы используете смартфон, тем более четко следует представлять риск и то, как его предотвратить. Смартфоны – мощные "излучатели информации". Они создавались специально для того, чтобы их владельцы были постоянно на связи, без проблем выходили в социальные сети. А ваши персональные данные – ценная информация, которую можно собирать, обрабатывать и даже продавать.

Крайне важно делать резервные копии. Потеря смартфона способна обернуться настоящей катастрофой, если нет резервной копии. Лучше делать "бэкапы" регулярно и хранить в надежном месте. Ну и, конечно, знать, как быстро восстановить данные в телефоне из резервной копии.

1.2. ПЛАТФОРМЫ И ОПЕРАЦИОННЫЕ СИСТЕМЫ СМАРТФОНОВ

В настоящее время самыми распространенными платформами для смартфонов являются Apple iPhone и Google Android. За ними — Blackberry и Windows. Важнейшее отличие Android: это система, главным образом, с открытым кодом. Принцип открытого кода позволяет независимым специалистам изучать программу и убеждаться, справляется ли она со своей задачей защиты пользовательских данных и коммуникаций. Это помогает делать платформу более безопасной. Смартфоны под управлением Android более "прозрачны" с точки зрения обеспечения безопасности данных и коммуникаций. Многие программисты, неравнодушные к вопросам безопасности, разрабатывают приложения для Android.

Устройства Blackberry всегда продвигались как "безопасные" для электронной почты и мгновенных сообщений. Причина в том, что сообщения и почта передаются по защищенным каналам между серверами Blackberry. У злоумышленника, задумавшего перехватить и прочитать такое сообщение, нет шансов. Но увы! Многие правительства сегодня хотят обеспечить себе доступ к этим коммуникациям. Предлоги — борьба с угрозой терроризма и организованной преступностью. Примеры таких стран — Индия, Объединенные Арабские Эмираты, Саудовская Аравия, Индонезия, Ливан. В этих странах владельцы Blackberry находятся под особым контролем, а правительства пытаются обеспечить себе доступ к их информации.

Заметная ниша современного рынка представлена так называемыми "функциональными телефонами" (feature phones). Примерами могут служить Nokia 7705 Twist и Samsung Rogue. Функциональный телефон — что-то среднее между обычным мобильным телефоном и смартфоном. Функциональный телефон обладает рядом возможностей смартфона, но, как правило, менее гибкой операционной системой и, как следствие, более узким набором средств обеспечения безопасности. Уровень безопасности сложно повысить.

Иногда смартфон продается под каким-то определенным брендом (например, оператора сотовой связи). Бывает, что купленный смартфон можно использовать только с этим оператором. СИМ-карты других операторов просто не будут опознаваться. В таких устройствах нередко можно увидеть программы, разработанные владельцем торговой марки. Некоторые функции заблокированы, другие, наоборот, добавлены. Идея

брендирования — сориентировать покупателя на определенную марку и получить больше прибыли. Но иногда владелец бренда собирает о владельцах таких смартфонов дополнительную информацию, а то и вовсе имеет доступ к устройствам.

Вот почему не стоит связываться с заблокированными устройствами. Если можете, покупайте обычный смартфон. Иначе ваша информация будет проходить через одного предопределенного провайдера, что значительно облегчает возможности контроля со стороны. Сменить СИМ-карту, чтобы использовать другие каналы коммуникаций, не получится. Если ваш смартфон заблокирован, обратитесь к специалисту, которому доверяете, чтобы он попробовал разблокировать устройство.

1.3. ОБЩИЕ МЕТОДЫ И СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

1.3.1. Общие настройки

У смартфонов много настроек для обеспечения безопасности. Важно понимать, как именно настроен ваш смартфон, какие установки безопасности смартфонов существуют, но по умолчанию не используются, и те, которые по умолчанию включены, но делают смартфон более уязвимым.

1.3.2. Установка и обновление программ

Обычное дело при установке программ на смартфон — использовать магазин iPhone App Store или Google Play. Пользователь входит (логин-пароль) в магазин, скачивает и устанавливает программу. (Многие программы бесплатны). Данные о том, что делает владелец аккаунта, сохраняются. Владельцы магазина могут следить за тем, какие страницы вы читаете и какие приложения выбираете.

Предполагается, что программы проверяются владельцами самих магазинов (Google или Apple). На деле это слабая защита от рисков, связанных с использованием разных программ. Например, некоторые приложения умеют копировать и отправлять данные из вашей адресной книги. На смартфонах Android всякое приложение перед установкой запрашивает для себя определенные права. Обращайте внимание, что именно хочет делать программа и насколько эти требования соответствуют ее предназначению. К примеру, если вы хотите установить программу для чтения новостей, а та вознамерилась отправлять контакты из вашей адресной книги какому-то постороннему лицу, есть смысл поискать другие, альтернативные программы.

Приложения для Android можно скачать из других источников, не только из официального магазина Google. Чтобы использовать их, нужно в настройках смартфона выбрать пункт "Приложения" и поставить галочку в поле "Неизвестные источники". Иные пользователи предпочитают именно альтернативные источники, чтобы свести к минимуму онлайновые контакты с Google. Одно из таких альтернативных программных хранилищ — F-Droid ("Free Droid"). Там размещаются только бесплатные программы с открытым кодом. Но, пожалуйста, скачивайте программы только с тех сайтов, которым доверяете. Если вы не чувствуете себя достаточно опытным пользователем, лучше ограничиться Google Play.

Бывает, что нет желания (или возможности) скачивать программы из интернета. Можно взять программу из смартфона друга. Для этого нужно, используя Bluetooth, переписать соответствующий файл *.apk* (сокращение от "пакет приложения Android"). Можно переписать файл .apk и на карточку microSD, и с помощью кабеля, подключив

смартфон к USB-порту компьютера. Когда файл будет на месте, просто нажмите и удерживайте — появится приглашение к установке.

1.3.3 Голосовая и текстовая связь

Смартфон умеет подключаться к интернету по сотовой сети или по wi-fi. Разговор можно сделать более безопасным, например, с помощью VoIP и дополнительных средств защиты. Некоторые программы для смартфонов умеют делать это и для обычных мобильных телефонов.

1.3.3.1. Skype

Самая популярная коммерческая программа VoIP. Skype доступен для всех платформ смартфонов и хорошо работает при надежном соединении wi-fi. Связь по каналам мобильных операторов обычно не так хороша для Skype.

Skype — программа без открытого кода. Очень трудно оценить, безопасен ли Skype на самом деле. Владельцем программы является корпорация Microsoft. Коммерческий интерес — знать, когда вы пользуетесь Skype и откуда. Наконец, Skype может дать правоохранительным органам доступ к истории ваших коммуникаций.

1.3.3.2. Другие программы VoIP

Обычно использование VoIP не предусматривает оплаты (или заметно дешевле звонков по телефону). Да и следов данных остается куда меньше. Возможно, защищенный звонок VoIP — самый надежный способ связи на сегодняшний день.

CSipSimple — мощный клиент VoIP для платформы Android. CSipSimple активно развивается, доступны удобные шаблоны настроек для разных служб VoIP.

Open Secure Telephony Network (OSTN) и сервер Ostel, поддерживаемый Guardian, — проект, который сегодня предлагает одно из самых безопасных средств голосовой связи. При использовании CSipSimple вы не связываетесь напрямую с вашим собеседником. Все данные проходят через сервер Ostel. Поэтому отследить ваш разговор и установить личность собеседников гораздо труднее. Кроме того, Ostel не хранит никакие данные (кроме логина и пароля, которые нужны для входа на сервер). Ваши разговоры шифруются. То же касается мета-данных, которые обычно весьма трудно спрятать. Установить программу и начать ею пользоваться весьма просто.

RedPhone — бесплатная программа с открытым кодом, которая шифрует голосовые коммуникации. Ее легко использовать, здесь те же понятия, что и в телефонной связи. Ваш собеседник, разумеется, тоже должен установить RedPhone. Для простоты RedPhone использует в качестве идентификатора номер вашего мобильного телефона (а не логин, как другие сервисы VoIP). Это удобно, однако создает дополнительные риски: становится проще отслеживать трафик и адресатов. В системе RedPhone используется центральный сервер, через который проходят все данные. Тот, кто контролирует сервер, вполне может контролировать сами данные.

1.3.4. SMS

SMS небезопасны по своей природе. Всякий, кто имеет доступ к мобильной телекоммуникационной сети, в принципе, может легко перехватывать сообщения. Так оно и происходит, причем довольно часто. В критической ситуации не следует полагаться на

небезопасные SMS. Нет способа определить подлинность SMS-сообщения. Нельзя сказать наверняка, прошло ли сообщение "как надо" или кто-то изменил содержание по пути. Удостовериться, что письмо отправлено именно тем, кто его подписал, тоже не получится.

TextSecure — бесплатная программа с открытым кодом для обмена SMS на смартфонах с ОС Android. Поддерживается шифрование сообщений. Можно использовать с TextSecure любое/привычное приложение для SMS. Для шифрования нужно, чтобы TextSecure был установлен на смартфонах отправителя и получателя. Программа автоматически определяет, когда на смартфон приходит сообщение, зашифрованное с помощью TextSecure. Также можно отправлять шифрованные сообщения сразу нескольким людям. Сообщения снабжаются цифровой подписью, поэтому каким-либо образом изменить их не получится.

1.3.5. Безопасный чат

Обмен мгновенными текстовыми сообщениями по смартфону создает дополнительный поток информации, который подвержен риску. Эти разговоры могут быть использованы злоумышленниками. Поэтому лучше быть особенно осторожным, когда набираете текстовые сообщения на смартфоне. Есть несколько способов повысить безопасность мобильного чата. Лучший — использовать шифрование на стороне и отправителя, и адресата. Вы будете уверены, что общаетесь именно с тем человеком, который нужен.

Для iPhone и Android-устройств можно рассмотреть приложение ChatSecure. Программа позволяет применить стойкое шифрование к текстовым сообщениям с помощью протокола Off-the-Record. ChatSecure — бесплатная программа с открытым кодом.

1.3.6. Хранение данных на смартфоне

Современные смартфоны — настоящие хранилища данных. К сожалению, доступ к этим данным получить довольно легко. Для этого даже необязательно держать само устройство в руках. Поэтому владельцу смартфона имеет смысл подумать об основных способах предосторожности. В частности, можно организовать шифрование всех ценных данных на вашем смартфоне с помощью специальных утилит.

1.3.6.1. Шифрование данных

Примером удобной программы для шифрования (и расшифровки) данных является Android Privacy Guard (APG). Эта утилита позволяет реализовать на Android-устройстве шифрование OpenGPG для файлов и e-mail. APG поможет защитить файлы и документы на телефоне, как и сообщения электронной почты.

1.3.6.2. Безопасное хранение паролей

Вы можете хранить все необходимые пароли в надежно защищенной базе. На компьютере для этого можно использовать программу Keepass. Для доступа к базе необходимо помнить пароль. С помощью Keepass вы можете использовать очень стойкие, надежные пароли, которые не потребуется запоминать. Кроме того, в программу встроен генератор паролей — вам не придется ломать голову и придумывать что-то по-

настоящему серьезное. На смартфоне под управлением Android можно использовать программу KeePassDroid — она работает с тем же форматом базы, что и Keepass. Рекомендуем хранить на мобильном устройстве только те пароли, которые вам действительно нужны в дороге. Лучше носить с собой маленькую базу самых необходимых паролей, чем копию всей вашей большой рабочей базы. Помните: поскольку доступ к базе защищен паролем, нужно использовать действительно сложный пароль, который нельзя угадать или подобрать.

1.3.7. Отправка e-mail со смартфона

В первую очередь решите для себя: так ли необходимо получать и отправлять электронную почту на смартфоне. Как правило, обеспечить безопасность компьютера проще, чем смартфона. Вероятность того, что смартфон будет украден или отобран, или его так или иначе станут "мониторить", выше, чем для компьютера.

Вот несколько советов, как снизить риск использования e-mail на смартфоне:

- Не полагайтесь на смартфон как на основное устройство для работы с e-mail. Не рекомендуем скачивать электронные сообщения с почтового сервера и хранить их исключительно на смартфоне. Убедитесь, что копии есть где-то еще.
- Если вы используете шифрование e-mail в общении с кем-либо из коллег или друзей, установите шифровальную программу не только на компьютер, но и на смартфон. Дополнительный плюс — ваши ценные сообщения на смартфоне окажутся зашифрованными и не будут доступны злодею, даже если сам смартфон окажется у него.

Хранить секретный (приватный) шифровальный ключ на мобильном устройстве может быть довольно рискованно. Но преимущество от возможности защищать почту шифрованием может перевешивать риск. Возможно, есть смысл создать отдельную пару шифровальных ключей для мобильного устройства, используя (APG). Таким образом, не придется копировать и хранить на смартфоне ваш "основной", рабочий секретный ключ. Правда, будет необходимо сообщить адресатам об этой ситуации с двумя ключами.

1.3.8. Фото и видео на смартфоне

Делать фотографии, видео- или аудиозаписи на смартфоне сегодня может любой. Важно, чтобы ценные материалы были надежно защищены. В частности, идентификация персонажа вашего видео может принести ему неприятности вплоть до угрозы жизни, если смартфон попадет в чужие руки. Вот некоторые советы:

- Отработайте порядок загрузки записанных материалов в какое-нибудь надежное онлайновое хранилище и удаления этих материалов со смартфона так быстро, как это возможно.
- Используйте программные средства размытия лиц на фото и видео и искажения голоса на аудиозаписях.
- Удаляйте мета-данные из отснятых материалов.

Команда Guardian Project создала бесплатную программу с открытым кодом ObscuraCam для распознавания и "замыливания" лиц на фотографиях. Вы можете даже выбирать, каким способом искажать изображения лиц. ObscuraCam позволяет удалять оригинальные фото, можно также настроить процедуру копирования сохраненных изображений.

1.3.9. Доступ к интернету со смартфона

Доступ к сайтам в интернете и публикация собственных материалов в онлайне, включая фото и видео, оставляют многочисленные следы. Это фактор риска. Использование смартфона повышает риск.

1.3.9.1. Доступ к сети по wi-fi или мобильную сеть

Смартфоны позволяют получать доступ к интернету по сотовой связи (GPRS, EDGE, UMTS, LTE — в зависимости от оператора) или по wi-fi (например, в интернет-кафе).

Если использовать анонимное подключение wi-fi, кажется, что смартфон оставляет меньше данных, чем при соединении через сотовую связь. Но иногда wi-fi не найдешь, и единственный способ связи — через сотового оператора. Увы, протоколы вроде EDGE или UMTS не являются открытыми. Независимые разработчики и специалисты по безопасности не могут со стопроцентной достоверностью сделать вывод о том, как именно тот или иной протокол используется тем или иным оператором.

В некоторых странах для операторов сотовой связи существует иное законодательство, чем для провайдеров доступа к интернету. Это может касаться простоты/сложности организации "прослушивания".

Повысить уровень безопасности можно, если использовать программы для обеспечения анонимности и шифрования данных.

1.3.9.2. Анонимность

Чтобы пользоваться интернетом анонимно, используйте Android-приложение Orbot. Эта программа направляет весь трафик через анонимную сеть Tor.

Другое приложение, Orweb, представляет собой веб-браузер "с акцентом на приватность". Совместное использование Orbot и Orweb позволяет анонимно ходить по сайтам в интернете, обходить веб-фильтры и межсетевые экраны.

1.3.9.3. Прокси

К мобильной версии браузера Firefox — Firefox mobile — можно добавить расширение прокси, которые будут перенаправлять ваш трафик через сервер-посредник (прокси). Оттуда трафик идет на сайт, который вам нужен. Этот "маневр" поможет в условиях цензуры. Тем не менее, сам факт обращения к прокси можно отследить, если только это обращение не зашифровано. Мы рекомендуем Proxy Mobile от Guardian Project, с помощью которого можно обеспечить функционирование защищенного механизма прокси.

1.4. ДОПОЛНИТЕЛЬНЫЕ СРЕДСТВА БЕЗОПАСНОСТИ

1.4.1. Полный доступ к возможностям смартфона

На обычным смартфоне установлены прошивка, операционная система и прикладные программы от производителя. Правда, некоторые предустановленные программы по умолчанию заблокированы, да так, что ни удалить, ни изменить. (Многие из этих функций пользователю никогда не понадобятся). Есть функционал, полезный в смысле

обеспечения безопасности данных и коммуникаций. С другой стороны, есть и такие программы, которые лучше бы удалить во избежания рисков.

Именно поэтому продвинутые пользователи ищут пути получения большего контроля над своими смартфонами. Вы могли слышать эти слова. Для Android-устройств говорят: "рут" (root). Для устройств iOS (например, iPhone, iPad) — джейлбрейк (jailbreak). Фактически эта процедура означает одно и то же: возможность устанавливать и удалять любые программы, полностью контролировать хранение данных, память и коммуникации.

ВНИМАНИЕ: подобная процедура требует умения и уверенности в себе. Она может оказаться необратимой. Пожалуйста, не забывайте, что:

- Существует риск превратить смартфон в "кирпич", то есть, сделать его полностью нерабочим.
- Если на смартфон еще распространяется гарантия производителя или продавца, эта гарантия наверняка будет утрачена.
- В некоторых странах описываемая процедура может оказаться незаконной.

Если, тем не менее, вы будете аккуратны, получение рут-прав может помочь сделать ваш смартфон гораздо более безопасным устройством.

1.4.2. Альтернативные прошивки

Прошивка — комплекс программ для конкретного устройства. Прошивка не заменяет операционную систему и обеспечивает базовые функции устройства — работу динамика, микрофона, камеры, сенсорного экрана, памяти, клавиш, антенны и др.

Если у вас устройство Android, есть возможность установить альтернативную прошивку, которая поможет полнее контролировать смартфон. Имейте в виду: чтобы установить альтернативную прошивку, нужно приобрести т.н. "рут-права".

Пример альтернативной прошивки для Android-смартфона — Cyanogenmod. Эта прошивка позволяет, в частности, удалять приложения на системном уровне (в том числе те, которые установлены производителем или оператором мобильной сети). Главное же — вы сократите число способов, которыми злоумышленники могут воспользоваться для отслеживания смартфона (например, когда данные без вашего ведома пересылаются вашему провайдеру).

Кроме того, Cyanogenmod включает приложение OpenVPN, весьма полезное с точки зрения обеспечения безопасности. VPN (Virtual Private Network) — один из способов обеспечивать направление трафика через прокси (см. ниже).

В Cyanogenmod можно использовать режим инкогнито (история ваших коммуникаций не записывается на смартфон).

Cyanogenmod имеет много других функций. Однако не все Android-устройства поддерживают эту прошивку.

1.4.3. Шифрование всего устройства

Если у вас есть рут-права на вашем смартфоне, вы можете зашифровать его целиком или создать на нем отдельный зашифрованный том и поместить туда данные, которые нужно защитить.

Программа Luks Manager позволяет шифровать данные на лету. Программа имеет приятный интерфейс. Рекомендуем установить Luks Manager перед тем, как записывать какую-либо важную информацию на смартфон, и хранить эти данные в зашифрованном томе.

1.4.4. Виртуальная частная сеть (VPN)

Виртуальная частная сеть (VPN) — зашифрованный тоннель в интернете между вашим устройством и сервером VPN. Тоннелем это называется потому, что, в отличие от других способов шифрования трафика (например, https), здесь речь идет о шифровании всех сервисов, протоколов и содержания сообщений. VPN настраивается один раз и может быть закрыта, когда вы захотите.

Обратите внимание, что весь ваш трафик перенаправляется через прокси или VPN-сервер. Теоретически, злоумышленнику достаточно иметь администраторский доступ к прокси, чтобы анализировать вашу активность. Очень важно аккуратно выбирать прокси или VPN-службу. Есть смысл пользоваться разными прокси и/или VPN, поскольку направление данных по разным каналам уменьшает шансы оказаться "под колпаком".

Рекомендуем использовать VPN-сервер RiseUp. Вы можете использовать RiseUp VPN на Android-устройстве после того, как установите прошивку Cyanogenmod (см. выше). Довольно легко можно настроить подключение к RiseUp VPN на iPhone.

1.4.5 Основные шаги обеспечения безопасности

1.4.5.1. Доступ к телефону

Шаг 1. Включите в настройках блокировку SIM-карты. Эта опция защиты потребует введения PIN-кода при каждом включении телефона.

Шаг 2. Включите блокировку экрана (*Настройки -> Конфиденциальность -> Настроить блокировку -> Блокировка экрана*). Это позволит защитить доступ к смартфону с помощью графического рисунка или пароля. Для большей безопасности лучше использовать вариант с паролем, поскольку длина пароля здесь не ограничивается. Подробнее о парольной защите можно почитать в главе нашего руководства **Как создавать и хранить надежные пароли**.

Шаг 3. Включите автоблокировку. Ваш телефон будет отключаться через определенное время (этот промежуток вы можете указать сами).

1.4.5.2. Шифрование устройства

Шаг 4. Если на смартфоне установлена операционная система Android версии 4.0 или более свежая, рекомендуем воспользоваться опцией *шифрования устройства* (поддерживается не всеми смартфонами). Вам понадобится защитить телефон с помощью пароля, как описано выше.

Примечание. Перед тем, как шифровать смартфон, убедитесь, что он полностью заряжен и подключен к источнику питания.

1.4.5.3. Настройки сети

Шаг 5. Посматривайте, чтобы режимы Wi-Fi и Bluetooth не были включены без надобности. Также важно, чтобы устройство не находилось понапрасну в режиме модема или точки Wi-Fi (*Настройки -> Беспроводные сети*).

Шаг 6. Если ваше устройство поддерживает функцию ближней бесконтактной связи (*Near Field Communication, NFC)*), то, скорее всего, эта функция будет по умолчанию включена. Если вам она не нужна, придется отключить вручную.

1.4.5.4. Настройки местоположения

Шаг 7. В меню *Настройки -> Местоположение* отключите определение координат по Wi-Fi и мобильным сетям.

Примечание. Включайте определение местоположения только когда это необходимо. Это уменьшит риск отслеживания вашего устройства, сократит передачу данных приложениями, работающими в фоновом режиме, и поможет сэкономить ресурс аккумулятора.

1.4.5.5. Блокировка приложений

Шаг 8. Порой знакомые просят ваш смартфон, чтобы посмотреть фотографии или быстро что-то найти в интернете. Отказывать неудобно, но вы не хотите, чтобы посторонние люди копались в личных файлах. Специально для таких случаев в Android 5.0 Lolipop появилась возможность заблокировать устройство в нужном приложении. Для активации функции нужно зайти в раздел *Безопасность — Блокировка в приложении — Вкл*. После этого в любом нужном приложении можно нажать кнопку «*Недавние*», а затем на иконку булавки. Приложение откроется, но из него нельзя будет выйти. Для разблокировки одновременно нажмите «*Назад*» и «*Недавние*», после чего введите PIN-код или пароль.

1.4.5.6. Менеджер паролей

Шаг 9. Любой интернет-пользователь имеет десятки, а то и сотни учетных записей на различных сайтах и сервисах. Однако мало кто может запомнить уникальный пароль для каждого из них, поэтому почти везде используется один и тот же пароль. Хорошо, что разработчики приложений уже позаботились о решении данной проблемы. Менеджеры паролей, такие как LastPass или 1Password, помогают пользователям генерировать и хранить любое количество паролей.

1.4.5.7. Двухфакторная аутентификация

Шаг 10. Постарайтесь максимально сократить риск утечки данных и воспользуйтесь функцией двухфакторной аутентификации везде, где это возможно. Большинство современных сервисов позволяют включить подтверждение авторизации по SMS. Таким образом, мошенники не смогут получить доступ к вашей учетной записи, если у них в руках не будет вашего мобильного телефона. Некоторые приложения позволяют обходиться и без SMS (например, Authy). Программа автоматически генерирует шестизначный код, который исчезает через 12 секунд. Использовать Authy можно со всеми сервисами, поддерживающими двухфакторную аутентификацию.

1.4.5.8. Умная разблокировка Smart Lock

Шаг 11. Все пользователи гаджетов знают, что блокировка экрана устройства добавляет дополнительный уровень безопасности от угроз в онлайне и оффлайне. Тем не менее, большинство игнорирует эту меру безопасности, потому что вводить PIN-код десятки раз в день может быть очень утомительно.

К счастью, разработчики Android 5.0 Lolipop придумали, как обойти надоедливые пароли без ущерба для безопасности. Функция Smart Lock позволяет разблокировать мобильное устройство 3 способами:

- надежные устройства — устройство разблокируется, когда поблизости находится знакомый Bluetooth или NFC-метка;
- безопасные места — разблокировка устройства по геолокации (например, дома или в офисе);
- распознавание лиц — устройство разблокируется, если гаджет «узнал» владельца.

Как включить Smart Lock:

- *Настройки — Безопасность — Блокировка экрана;*
- выберите один из способов блокировки экранов (кроме «Провести по экрану»);
- перейдите в конец списка, найдите пункт Trust Agents и активируйте Smart Lock;
- вернитесь в начало раздела «*Безопасность*» и откройте меню Smart Lock;
- выберите один из вариантов умной разблокировки, перечисленных выше.

1.4.5.9. Android VPN-client

Шаг 12. Вопреки рекомендациям экспертов по кибербезопасности, пользователи часто подключаются к публичному Wi-Fi в кафе, аэропортах, отелях и других местах. Таким образом, у злоумышленников появляется шанс перехватить важные личные данные, в том числе логины и пароли от интернет-банкинга.

Дополнительной мерой защиты может стать использование VPN-клиентов, которые шифруют трафик вашего устройства, а также скрывают IP-адрес и местоположение. Если вы вынуждены часто использовать публичные беспроводные сети (например, в путешествиях или командировках), то воспользуйтесь одним из приложений: Hotspot Shield VPN, TunnelBear VPN или SuperVPN.

1.4.6. Практические советы

1) Держите сотовый телефон при себе. Не оставляйте его вне поля зрения и не давайте другим людям "попользоваться".
2) Включите стандартную защиту — запрос PIN-кода. Держите PIN-код в памяти, не записывайте на бумажку, вложенную в кошелек или паспорт. Используйте свой пин-код, а не значение по умолчанию.
3) Пометьте каким-нибудь способом SIM-карту, карточку памяти, аккумулятор и корпус самого телефона. Это придаст вам уверенность, что телефон никем не разбирался.
4) Если приходится ремонтировать телефон, или вы решили его подарить/продать, не забудьте вынуть сим-карту и карту памяти, а также очистить адресную книгу, список SMS и прочие разделы.
5) Когда устанавливаете новую сим-карту, позаботьтесь о том, чтобы никакие данные не "застряли" на предыдущей.
6) По возможности выбирайте только тех операторов связи и магазины/продавцов, которые пользуются (более-менее) солидной репутацией.

7) Не забывайте делать резервные копии всех данных, копируйте их на компьютер. Позаботьтесь о том, чтобы данные хранились в безопасном месте.
8) Каждый аппарат имеет 15-значный уникальный код (IMEI). Он однозначно идентифицирует телефон. В большинстве моделей узнать IMEI можно, набрав *#06#. Код может быть написан на корпусе под аккумулятором. Запишите этот код и храните отдельно от телефона. Знание кода может послужить доказательством того, что аппарат действительно принадлежит вам.
9) Можно зарегистрировать телефон у оператора связи. В случае пропажи аппарата его использование нетрудно блокировать.
10) Звоните из разных мест. Когда мы делаем звонок по мобильному телефону, аппарат устанавливает связь с ближайшими сотовыми вышками. Таким образом, оператор сотовой связи, в принципе, знает точное местонахождение телефона. Пока телефон включен, он поддерживает контакт с вышками сотовой связи, даже если по телефону не разговаривают.
11) Если позволяют законы страны, покупайте сим-карту без регистрации, предоставления документов и заполнения анкет.
12) Не платите за мобильную связь кредитной карточкой. Такие карточки всегда именные.
13) Телефон может работать как диктофон. Некоторые аппараты можно включить в таком "диктофонном режиме" на расстоянии. А значит, без ведома владельца. Причем так, что с виду телефон будет выключен. Никогда не давайте свой телефон людям, которым вы не очень доверяете.
14) Во время важных встреч, на которых могут обсуждаться разные деликатные моменты, выключайте аппарат и вынимайте батарею. Или вообще не берите телефон с собой, если можете оставить его в безопасном, надежном месте.
15) Убедитесь, что ваш собеседник придерживается тех же правил безопасности, что и вы.
16) Не забывайте, что, пользуясь телефоном в публичных местах, где вокруг толпятся люди, а из-за шума вам порой приходится повышать голос, вы рискуете стать объектом обычной прослушки. К тому же в толчее телефон проще украсть.
17) Как правило, и голосовые, и текстовые мобильные коммуникации не могут похвастать высоким уровнем защиты (шифрования). Для защиты нужно использовать дополнительные безопасные криптографические программы у себя и у собеседника.
18) Если нужно отправить информацию так, чтобы она гарантированно не попала в чужие руки, вряд ли стоит полагаться на SMS. Этот способ текстовых коммуникаций не обеспечивает конфиденциальность. Кроме того, "смску" можно изменить или подделать. Очень часто SMS-сообщения образуют в памяти телефона целый архив. Если кто-нибудь украдет ваш телефон или просто получит к нему доступ, он сможет прочесть эти сообщения. Выработайте привычку удалять "смски" сразу после прочтения. В некоторых моделях телефонов можно отключить запись информации о телефонных звонках и SMS. Проверьте, есть ли в вашем аппарате такая опция.
19) Не храните конфиденциальную информацию в телефоне. Фотографии, видеозаписи, SMS. Как только предоставляется возможность, перемещайте их на компьютер, в безопасное хранилище.
20) Почаще стирайте записи о телефонных звонках, сообщениях, ненужные (необязательные) контакты в адресной книге, и так далее.
21) Если вы хотя бы иногда выходите в интернет с мобильного телефона, по возможности пользуйтесь для передачи данных "защищенным" протоколом SSL.
22) Подключайте телефон к компьютеру, только если твердо уверены, что оба устройства свободны от вирусов и другого вредоносного кода.

23) Не скачивайте и не устанавливайте в телефон незнакомые и непроверенные программы, рингтоны (мелодии звонков), обои (графическое оформление), Java-приложения и вообще что бы то ни было из источников, чья надежность не подтверждена.
24) Приложение Android Device Manager позволит вам быстро найти потерянный гаджет. С его помощью можно установить громкость рингтона на максимум, даже если устройство было в беззвучном режиме.