ПАМЯТКА

Публикация № 080703/b/1

Безопасная работа в беспроводных сетях

Как защититься от вторжения и кражи информации?

Большинство современных мобильных телефонов, коммуникаторов, переносных компьютеров и других портативных вычислительных устройств и средств связи могут обмениваться данными через инфракрасный порт (IrDA), беспроводные сети Bluetooth и WiFi. Аналогичными функциями могут также обладать стационарные компьютеры, переносные аудио/видео проигрыватели и другие устройства.

Зачастую соответствующие функции вашего устройства включены по умолчанию и не защищены должным образом от использования злоумышленниками. Владелец устройства, оснащенного функцией беспроводного обмена данными, может не подозревать, что злоумышленники имеют доступ ко всему содержимому его устройства, включая личные файлы, например адресную книгу мобильного телефона.

Следующие советы помогут защитить устройства с функцией беспроводного обмена данными от доступа со стороны злоумышленников, и предотвратить уничтожение, изменение или кражу ими ценной или конфиденциальной информации.

1. Познакомьтесь со своим устройством поближе

Многие владельцы устройств не осведомлены обо всех их функциях. Внимательно изучите технические характеристики своего устройства; узнайте, какими функциями беспроводного обмена данными оно обладает, как включаются, настраиваются и отключаются эти функции. Инструкция к устройству должна содержать исчерпывающую информацию по этому вопросу.

2. Все ли функции вам нужны?

Решите, какие функции беспроводной передачи данных своего устройства вы будете использовать и отключите неиспользуемые. Возможно, вы сочтете целесообразным отключить все эти функции, и включать их только на время использования – это существенно повысит безопасность использования устройства.

3. Защитите свое устройство паролем

Даже если вы отключили функции беспроводной передачи данных, ограничьте доступ к ним с помощью пароля (если это предусмотрено производителем устройства). Если производителем устройства уже был установлен такой пароль, смените его на свой собственный; периодически меняйте свой пароль. Инструкция к устройству должна содержать исчерпывающую информацию по этому вопросу.

Примите во внимание, что некоторые устройства позволяют установить только относительно слабый пароль, который может быть легко найден злоумышленником путем полного перебора возможных вариантов.

4. Защитите свое устройство межсетевым экраном

Некоторые устройства могут быть оснащены встроенным межсетевым экраном (firewall) или иной программой фильтрации принимаемых и передаваемых данных, либо позволять установку таких программ. Межсетевой экран поможет обеспечить защиту от несанкционированных подключений по протоколу WiFi, а иногда и через Bluetooth. Инструкция к устройству должна содержать исчерпывающую информацию по этому вопросу.

5. Используйте весь потенциал защиты устройства

Протокол WiFi предусматривает наиболее высокую степень защиты среди протоколов беспроводной передачи данных. Наиболее совершенной версией стандарта защиты протокола WiFi на сегодня является WPA2, за ним по убывающей идут WPA и WEP. Используйте наиболее защищенный из поддерживаемых вашим устройством стандартов защиты.

Отключите рассылку идентификатора своего устройства (SSID broadcast), запретите доступ к настройкам подключения и самого устройства по беспроводной связи, а также «гостевой доступ» (guest login).

Измените идентификатор своего устройства (SSID), установленный его производителем, на свой собственный, и задайте пароль доступа к устройству через беспроводное подключение. Инструкция к устройству должна содержать исчерпывающую информацию по этому вопросу.

Примите во внимание, что используемые в вашем устройстве стандарты защиты обмена данными могут превзойти возможности некоторых сетей WiFi, или, напротив, оказаться недостаточными для работы в некоторых из них. Старайтесь подключаться только к наиболее безопасным из доступных сетей. Веб-сайт администратора сети WiFi может содержать сведения о поддерживаемых сетью стандартах защиты и инструкции по настройке устройств для работы в этой сети.

6. Подумайте о дополнительной защите

Если ваше устройство содержит особо ценную или конфиденциальную информацию, подумайте над обеспечением дополнительной защиты. В зависимости от возможностей устройства, ею может стать хранение информации в разделе встроенной памяти, недоступном через беспроводную связь, защита паролем доступа к отдельным разделам встроенной памяти устройства, шифрование информации и т.д. Инструкция к устройству должна содержать исчерпывающую информацию по этому вопросу.

7. Не разрешайте подключение без запроса

Если это возможно, настройте свое устройство таким образом, чтобы беспроводная связь с другими устройствами устанавливалась не автоматически при поступлении от них запроса, а только после подтверждения желания установить связь с вашей стороны. Разрешайте подключение без запроса лишь в крайних случаях, например для установления доверительных отношений (pairing) между двумя принадлежащими вам устройствами, поддерживающими стандарт Bluetooth. Инструкция к устройству должна содержать исчерпывающую информацию по этому вопросу.

8. Регулярно избавляйтесь от мусора

Обычно в вашем устройстве сохраняются «профили подключения» к сетям WiFi, с которыми вы когда-либо работали. Чем больше таких профилей хранится в вашем устройстве, тем выше вероятность несанкционированного доступа к нему. Регулярно удаляйте профили тех сетей, которыми вы уже не пользуетесь. Инструкция к устройству должна содержать исчерпывающую информацию по этому вопросу.

9. Будьте особенно осторожны при работе в публичных сетях

Публичные сети WiFi, к которым может бесплатно подключиться любой желающий, доступны сегодня во многих аэропортах, гостиницах, кафе и других общественных местах. Часто такие сети бывают недостаточно защищены от перехвата передаваемой через них информации.

При необходимости подключения к такой сети, старайтесь использовать подключение через «виртуальную частную сеть» (VPN) и пользоваться защищенным протоколом доступа к веб-сайтам – Secure HTTP (HTTPS). Инструкция к устройству может содержать необходимую информацию по этому вопросу, дополнительная информация может быть доступна на веб-сайте администраторов публичных сетей.

10. Старайтесь избегать передачи важной информации

Даже наиболее защищенные беспроводные сети потенциально более уязвимы к перехвату передаваемой информации, чем проводные. Не передавайте без крайней необходимости по беспроводным сетям ценную или конфиденциальную информацию.

Злоумышленники также могут перехватить в беспроводных сетях пароли, используемые вами для доступа к веб-сайтам, электронной почте и другим сетевым ресурсам. Впрочем, вероятность этого (хотя и меньшая) существует и в проводных сетях.

11. Не забывайте об обновлениях

Многие современные устройства допускают обновление установленного на них программного обеспечения и микрокода (firmware), который управляет работой устройства. Обновления могут повысить степень защищенности устройства и исправить ошибки, допущенные в предыдущих версиях обновляемых программ или микрокода. Обычно такие обновления можно бесплатно загрузить с веб-сайта производителя устройства.

Будьте внимательны при установке обновлений и следуйте прилагаемой инструкции, так как отступление от нее может привести к неработоспособности устройства или потере хранящейся в нем информации.

Установку обновлений также можно произвести в сервисных центрах производителя устройства, которые могут взимать за это плату. Инструкция к устройству должна содержать исчерпывающую информацию по этим вопросам.