 **ЦИФРОВОЙ МИР: НАДЕЖНЫЕ СМАРТ-УСТРОЙСТВА**

**ЧТО ТАКОЕ СМАРТ-УСТРОЙСТВО?**

Смарт-устройство («умное», «интеллектуальное» устройство) способное подключаться к другим устройствам, обмениваться с ними данными, взаимодействовать с ними и со своим пользователем.

Самые популярные среди потребителей смарт-устройства - это смартфоны, игровые приставки, смарт-телевизоры, портативные трекеры состояния здоровья (например, фитнес-трекеры), термостаты, детские игрушки и оборудованные доступом в Интернет автомобили. Все эти продукты способны собирать и анализировать пользовательские данные и передавать их на другие подключенные к сети устройства.

**Сети, состоящие из подключённых друг к другу смарт-устройств, называются Интернетом вещей (IoT).**

Смартфоны - один из самых популярных видов интеллектуальных устройств, так как помимо текстовых сообщений и звонков они способны выполнять множество других функций: шагомера, геолокатора и даже измерителя пульса. Кроме того, смартфон можно сделать центральным хабом, который обеспечивает взаимодействие пользователя с другими интеллектуальными устройствами, такими как принтеры, акустические системы, домашние системы безопасности или фитнес-трекеры.

Смартфоны играют особую роль для потребителей где доступ к Интернету через стационарное широкополосное подключение из дома весьма ограничен. Потребители используют смартфоны для осуществления платежей, отправки и получения денежных переводов, связи, доступа к заработной плате, кредитам т. п. - то есть для выполнения важнейших функций. Это означает, что обеспече ние доступности, безопасности и защищенности подключенных к Интернету телефонов особенно важно для потребителей, использующих свои смартфоны для получения основных услуг.

Другими наиболее популярными смарт-устройствами являются системы безопасности умных домов и интеллектуальные устройства мониторинга состояния здоровья.

Фитнес-трекеры следят за уровнем активности пользователя, характером его сна и частотой сердечного ритма, помогая анализировать текущее состояние здоровья.

Системы безопасности умных домов включают в себя беспроводные камеры, замки и датчики движения. Если эти устройства регистрируют в доме необычную активность, они направляют на смартфон владельца соответствующее оповещение.

Растёт количество умных продуктов, предлагающих индивидуальные решения людям с ограниченными возможностями. Например, это умные часы для людей с потерей зрения. Такие устройства вибрируют при получении входящих электронных сообщений и переводят их в шрифт Брайля на лицевой панели часов. Умные лампочки, подключенные к дверному звонку или телефону, облегчают жизнь людям с потерей слуха.

Вовлечение в жизнь людей все большего количества умных устройств требует внимания к сопутствующим проблемам безопасности и конфиденциальности, ставит вопрос о необходимости разработки новых механизмов защиты потребителей для обеспечения их доверия к этим устройствам.

**ПРОБЛЕМЫ СМАРТФОНОВ И ДРУГИХ СМАРТ-УСТРОЙСТВ**

**Безопасность:** Все интеллектуальные устройства являются частью более крупных подключенных систем и сетей, оттого уязвимость любой отдельно взятой части может поставить под угрозу всю систему.

Зачастую IoT-устройства отличаются слабой защитой, которую очень просто взломать. Этим с удовольствием пользуются преступники. В последние годы происходят громкие кибератаки, запущенные хакерами, которые получили доступ к незащищённым потребительским устройствам. Помимо рисков нарушения работы сетей и сервисов, незащищенные смарт-устройства ставят под угрозу безопасность самих потребителей. Исследователи выявили, что устройства можно взламывать и управлять ими удаленно - в одном из случаев специалисты в области компьютерной безопасности смогли получить доступ к подключенному к сети автомобилю и управлять его рулевой системой, тормозной системой и дверными замками.

**Защита личных данных:** Проведенное в 2018 году глобальное потребительское исследование показало, что 52% пользователей за год стали сильнее беспокоиться о своей конфиденциальности в Интернете. При этом 43% респондентов другого опроса заявили, что хотели бы узнать больше о данных, собранных о них с помощью подключенных устройств, а 47% респондентов были обеспокоены возможностью кражи личных данных. Значительный риск с точки зрения сохранения конфиденциальности данных возникает из-за того, что устройства могут и конструктивно предназначены для обмена данными друг с другом, способны автономно передавать данные третьим сторонам. Объекты внутри подключенной системы могут собирать данные или информацию, которые сами по себе безвредны, но при сопоставлении и анализе вместе с другими данными способны раскрыть достаточно точные сведения о личности, что приводит к расширению возможностей по отслеживанию пользователей и их профилированию.

Взломав защиту безобидных бытовых приборов, злоумышленник может начать шпионить за их владельцем — например, подслушивать разговоры или подглядывать за владельцем через IP-камеру.

**Функциональная совместимость:** Обеспечение того, чтобы различные умные устройства, которыми владеют потребители, могут обмениваться данными друг с другом, также очень важно для потребителей с точки зрения максимально эффективного использования устройств. Если вы купили «домашний помощник» и обнаружили, что он не может подключиться к другим устройствам в вашем доме, это серьезно ограничит его функциональность. Если устройства могут эффективно работать только с другими гаджетами от той же компании, потребитель оказывается вынужденно привязанным к одной системе, а это ограничивает его выбор и конкуренцию на рынке.

**Обновления функций безопасности**: Общая проблема с подключенными устройствами - это отсутствие обновлений функций безопасности. Если обновления недоступны, устройства могут стать уязвимыми для вирусов и кибератак. Тем не менее, компании не обязаны предоставлять обновления, и кроме того, нигде не оговаривается, как долго они должны предоставлять такие обновления для устройств старых моделей.

**За получением подробной консультации и правовой помощи  потребители**

**могут обращаться:**

— в Общественную приемную Управления Роспотребнадзора по Новгородской

области по телефонам 971-106;

— в Центр по информированию и консультированию потребителей  ФБУЗ «ЦГи Э

в Новгородской области» по телефону 77-20-38, 73-06-77;

Е-mail: [zpp.center@yandex.ru](mailto:zpp.center@yandex.ru); ВК: vk.com|zppnovgorod

— на «горячую линию» Единого консультационного центра Роспотребнадзора,

который функционирует в круглосуточном режиме, телефон 8 800 555 49 43

(звонок бесплатный).

**Кроме того,** на государственном информационном ресурсе в сфере защиты прав потребителей <http://zpp.rospotrebnadzor> вы можете найти памятки, образцы претензий, исковых заявлений и другую полезную информацию для потребителей

Данная статья подготовлена Центром по информированию и консультированию потребителей на основе источников:

1) http://konfop.ru/тема-всемирного-дня-прав-потребител/

2)https://blog.colobridge.net/2017/11/worldwide-iot-statistics/

3)https://www.kaspersky.ru/blog/internet-of-vulnerabilities/19265/

4) <https://techrocks.ru/2018/12/11/internet-of-things-privacy-requirements/>