

Жители Тверской области все чаще покупают «умную» технику, которой можно управлять со смартфона, но порой забывают об элементарных правилах безопасности

«Умные» устройства и «кухонные» хакеры

Исследовательская компания GfK выяснила, что в 2018 году в России было продано 1,2 млн «умных» устройств. Это на 33% больше, чем годом ранее. Расходы на «умную» технику выросли на 11% и составили 20,8 млрд рублей.

Россияне охотно покупают телевизоры, холодильники, стиральные машины и другую технику, которой можно управлять со смартфона. Быстрыми темпами растут продажи камер наблюдения, «умных» лампочек и розеток, которыми можно управлять со своего мобильного. С каждым годом в нашей стране растет количество «умных» домов, в которых удаленно можно регулировать температуру и влажность воздуха, освещение и другие ресурсы.

Пока больший объем «умной» техники приходится на современные холодильники, стиральные машины, кондиционеры и телевизоры. Мобильные приложения дают возможность удаленного управления устройствами и их гибкой настройки. Например, некоторые функции современного телевизора проще настроить со смартфона, чем с помощью пульта.

Наиболее динамично растут объемы продаж IP- и Wi-Fi-камер. Их продажи у разных игроков рынка выросли в 20-30 раз в среднем по стране. Тверь не стала исключением. Многие компании продают коробочные решения для организации видеонаблюдения дома, в которое входят облачное хранение и управление данными. Этот рынок тоже стремительно развивается, но пока многие граждане самостоятельно тестируют «умные» камеры в домашних условиях.

— Количество «умных» устройств с каждым годом будет расти. И все они хотят получить от нас, пользователей, право на вы-



ход во внешний мир. Иногда эти устройства покупаются не в России, а напрямую в Китае через специализированные магазины, которыми пользуются многие жители Твери. Насколько безопасна такая покупка? — задается вопросом эксперт в сфере информационной безопасности, бывший сотрудник МВД Вячеслав Сапунов. — Многие «умные» устройства делают небольшие компании, которые в последнюю очередь уделяют внимание вопросу безопасности. Этим пользуются злоумышленники. Сейчас продается много устройств со слабой защитой или уязвимостями. А некоторые недобросовестные производители могут оставлять в них закладки, которые позволяют им потом получить доступ к этим устройствам.

Ради эксперимента на одном подобном гаджете Вячеслав Сапунов оставил заводской пароль. Через несколько дней к устройству подключились пользователи из Китая. Они просканировали сеть с целью найти возможность получить доступ к Wi-Fi роутеру и другим устройствам, которые к нему подключены.

Хакеры постоянно тестируют мировую паутину на предмет уяз-

вимостей и охотно делятся друг с другом данными. Взломав хотя бы одно из ваших устройств, злоумышленник может шаг за шагом захватить все гаджеты, подключенные к Интернету. Чем это опасно? Во-первых, если на вашем компьютере и телефоне подключен «мобильный банк», ваши деньги могут украсть. Во-вторых, в общий доступ могут попасть ваши персональные данные, в том числе фото, видео, платежные документы и личная переписка в социальных сетях и мессенджерах. В-третьих, хакеры могут использовать ваши устройства для своих грязных дел. Например, для массовых дос-атак на нужные им сайты. И вы даже можете не заметить, что ваш компьютер задействован в чьей-то многоходовке. И, в-четвертых, хакеры могут вывести вашу «умную» технику из строя.

Чтобы защитить себя, нужно своевременно обновлять прошивку и программное обеспечение всех своих устройств, в том числе смартфонов и Wi-Fi роутеров. Важно менять заводские пароли всех гаджетов, ставя свои — длинные и сложные. Очень желательно на каждое устройство иметь свой пароль. Если вы используете один

пароль на всю «умную» технику, то вы представляете для хакеров шикарную возможность получить доступ ко всей вашей информации. Пользуйтесь лицензионным программным обеспечением, в том числе для мобильных устройств. Для защиты Wi-Fi можно сформировать «белый список» устройств, которые имеют право подключаться к роутеру.

— Защитите смартфон, на котором стоит мобильный банк. Своевременно его обновляйте, а также не ставьте сомнительные программы, темы и игры, — говорит Вячеслав Сапунов. — Обращайте внимание на то, доступ к каким данным запрашивает приложение, которое вы только что установили. И если приложение вызывает сомнения, лучше не ставьте его.

Многие читатели могут возразить, что они не интересны хакерам, поэтому нет необходимости обращать внимание на безопасность. Но это далеко от истины. Сейчас разработаны целые инструменты, которые направлены на поиск уязвимостей у всех устройств, которые подключены к Интернету.

— Растет количество «умных» устройств с низкой степенью за-

щиты. И если раньше для взлома требовались определенные знания и навыки программирования, то сейчас достаточно нажать пару кнопок в специальной программе и получить результат, — рассказывает Вячеслав Сапунов. — Растет количество молодых людей, которые используют это программное обеспечение. Я их называю «кухонными хакерами». Только хочу напомнить, что взлом устройств и программ — это уголовно наказуемое преступление.

Впрочем, не только простые пользователи, но и бизнес проявляет беспечность. Вячеслав Сапунов при нашем корреспонденте протестировал 12 роутеров на одной из центральных улиц Твери и нашел три со слабой защитой. Если их взломает какой-нибудь злоумышленник, то он получит доступ ко всему трафику этих роутеров, а в перспективе и к устройствам, которые к нему подключены или подключатся в будущем.

— В начале нулевых годов в Твери почти никто не задумывался о безопасности. Многие ресурсы, даже различных государственных структур и ведомств, практически не были защищены, — вспоминает Вячеслав Сапунов. — И сейчас во многих крупных сетях, которые существуют в офисных центрах, часто важные данные защищены плохо или не защищены вовсе.

Информационная безопасность — это совсем не сложно. В Сети много полезной информации по этому поводу. Защита своих гаджетов должна стать полезной привычкой, как чистка зубов перед сном. Соблюдение простых правил позволит сохранить в безопасности ваши «умные» устройства и данные.

Андрей САБЫНИН

НОВЫЕ ТЕХНОЛОГИИ

Братья-инженеры из Твери создали холодильник с новой схемой работы

Физики Алексей и Дмитрий Карпенковы из Твери разработали новую технологию охлаждения — магнитную, которая может применяться в холодильниках

В основе разработки — твердотельная магнитная система, по энергоэффективности превосходящая механизмы обычных холодильников на 30-40%. В новом холодильнике использован магнетокалорический эффект, заключающийся в том, что магнитный материал меняет свою температуру при намагничивании.

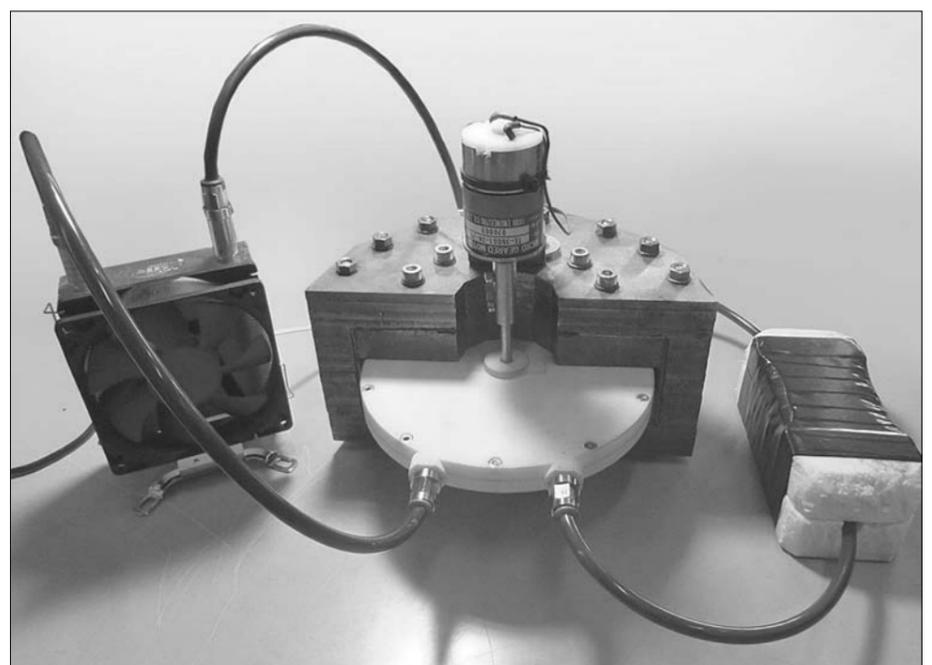
«Сам эффект не новый, над ним работают еще с

XIX века, а ныне занимаются все флагманы холодильного оборудования, — рассказал Алексей Карпенков, доцент кафедры физики конденсированного состояния Тверского государственного университета. — Уже создан холодильник для вина с магнитным охлаждением — но там нужно просто поддерживать заданную температуру. Основной недостаток системы — дороговизна».

Карпенков уточнил, что их с братом разработка (Дмитрий сейчас работает в московском университете МИСиС) — это новая реализация каскадного цикла охлаждения. Большой холодильник с таким эффектом из-за ограниченного финансирования создать

пока не удастся — но создан прототип. Разработчики будут пробовать реализовать его в промышленности и разговаривают об этом с производителями — как отечественными, так и зарубежными. Правда, россияне, по словам Карпенкова, не хотят рисковать и мало вкладываются в развитие технологий.

Энергоэффективность такой системы важна, поскольку обычные холодильники — самая «прожорливая» техника в квартире. И возможный дефицит энергоносителей в ближайшем будущем при отсутствии прогресса в энергоэффективности может негативно сказаться в том числе и на окружающей среде.



Прототип охлаждающего механизма. Фото: Дмитрий Карпенков, НИТУ «МИСиС».