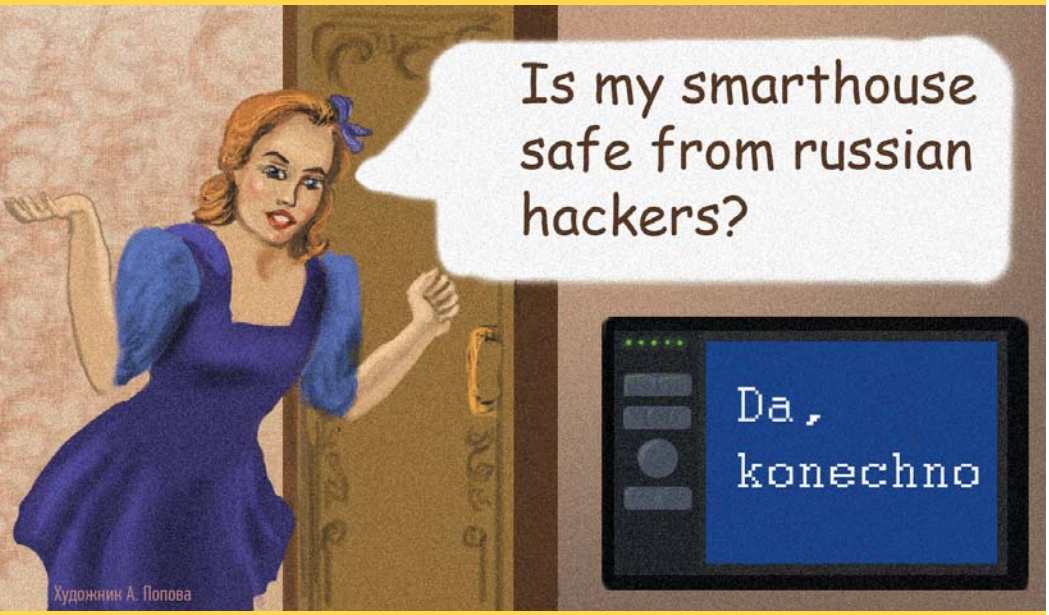


ДОМ НА ГРАНИ БЕЗУМИЯ

ЕКАТЕРИНА ТРОФИМОВА
ekaterina.trofimova@fsmedia.ru

В какой степени мы можем доверять вещам? Получившие доступ в Интернет, не задумают ли они заговор против людей? До какой степени вещи управляемы? Насколько наша жизнь станет менее предсказуемой и отчасти неконтролируемой, если концепция «Интернет вещей» всерьез и полноценно войдет в нашу жизнь? Об этом стоит поговорить.

Основная заповедь технической религии гласит, что механизмы делают именно то, для чего они придуманы. Но так ли оно в реальности? Не получится ли, что чем «умнее» вещь, тем быстрее наступит предел нашей власти над ней и тем больше мы начнем от нее зависеть? Умные вещи требуют особого ухода и внимания, и уж тем более постоянного и тщательнейшего контроля над ними.

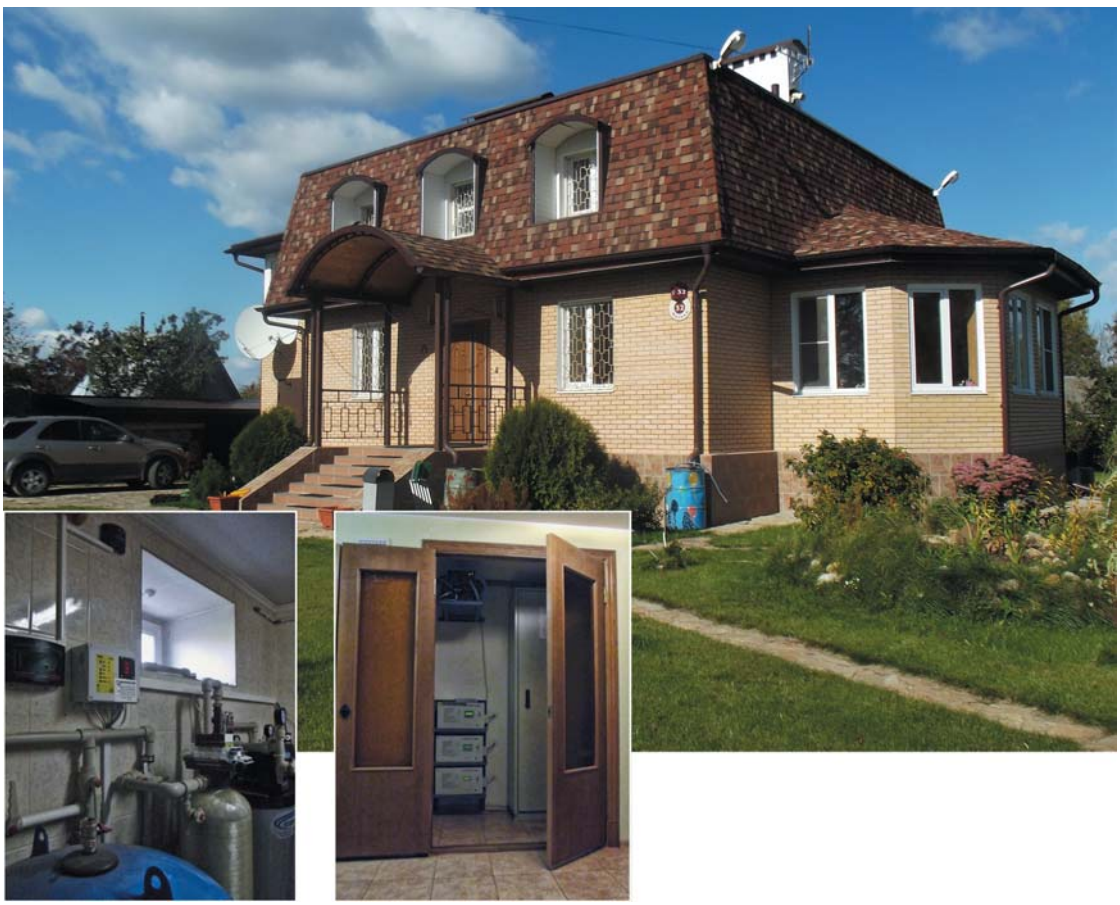
Сейчас в управлении «умным» домом основная ставка делается на передачу различных (тревожных или ситуационных, контрольных/требующих вмешательства хозяина и т. д.) сообщений на мобильное устройство пользователя. Но, думаю, мы все способны понять (если задумаемся), насколько это ненадежно.

К сожалению, «иммунитет» мобильников очень слаб. Еще лет десять назад главный «вирусолог» страны Евгений Касперский утверждал, что «те, кто зарабатывает сейчас на создании вирусов для ПК, начнут их модифицировать под мобильные телефоны. Ситуация трудно прогнозируема. Все зависит от того, как поведут себя производители ПО для смартфонов: оптимистический сценарий возможен только в случае, если они вплотную займутся вопросами безопасности. В ближайшем будущем возможно появление вредоносных программ, которые, используя дыры в ПО, смогут позвонить на другой телефон, записать или украсть какую-то информацию. Так что бойтесь!». В те времена наиболее уязвимым считался Nokia 6620. Первый вирус для него (Cabir) появился в 2004 г., но он не представлял большой опасности, поскольку поражал только некоторые мобильные телефоны с Bluetooth и не причинял особого вреда, ибо его разработали исключительно с целью доказать, что создать вирус для мобильных телефонов вполне возможно. Евгений Касперский тогда считал, что «пока нет смысла разрабатывать защиту — серьезный вирус всего один, стратегия развития индустрии пока неизвестна, и трудно представить, какие виды атак предпримут через год-два вирусописатели». Но уже тогда существовал вирус CommWarrior (Comwar), который был способен распространяться не только через протокол Bluetooth, но и через службу обмена сообщениями MMS. А поскольку обмен MMS — достаточно популярный сервис, прогнозы по поводу темпов распространения этого вируса выглядели тогда пугающе. Микко Хиппонен, директор департамента антивирусных исследований финской компании F-Secure, уже тогда сравнивал MMS-вирусы с почтовыми «червями» типа Bagle, Mydoom, Sobig: «MMS-зараза может распространиться по миру в считанные часы. С учетом этого она намного опаснее».

Возможно, для кого-то проблема вирусного заражения мобильников представляет всего лишь академический интерес. Но давайте вернемся с небес на землю.

Представим себе, что мы с мобильника удаленно осуществляем контроль за системами жизнеобеспечения нашего «умного» дома. А если мобильник заражен, нет никакой гарантии, что все под контролем, что никакой злоумышленник не повысит, к примеру, до критической температуру в нашей сауне или не устроит в детской комнате в наше отсутствие концерт «Рамштайна» во все возможные децибелы. Но оставим в покое мобильник, служащий пультом управления, — это всего лишь одно из слабых мест «умного» дома. Если задуматься всерьез, можно найти несчетное количество «дыр» и угроз четкой работе интеллектуальных систем, особенно при реализации новомодной концепции «Интернет вещей». Так «неужели в самом деле все сгорели карусели», и обеспечение надежности работы сложнейших систем «умного дома», требующих управления по сети, — утопия? Послушаем специалистов.

Александр Мелешкин, зам. директора Дирекции по информационным технологиям ЗАО «Издательство «7 Дней», полагает, что реальная угроза «бунта вещей», подключенных к Интернету, существует, но только если ее «заложили» специально или по недосмотру. Вероятность выхода из повиновения повышается при более универсальном (гибком) подходе при создании «разума» этих вещей. По его мнению, наиболее вероятными причинами такой ситуации скорее всего могут стать ошибки разра-



◀ Умный дом Юлии Раевской

ботчика, который не предусмотрел какой-либо сценарий развития ситуации в работе вещи или оставил незакрытой потенциальную уязвимость, которую обнаружат хакеры и найдут способ ею воспользоваться.

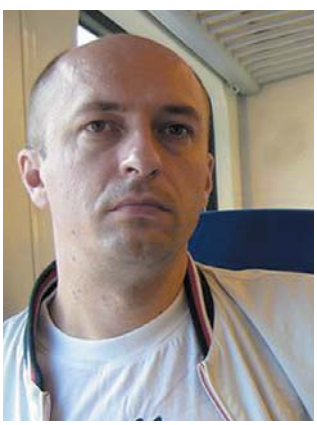
Александр Большев, аудитор службы информационной безопасности компании Digital Security, отчасти согласен с предыдущим высказыванием. По его мнению, сначала необходимо определить, что подразумевается под «бунтом вещей»: отказ системы, невозможность выполнять заложенные функции или некорректное выполнение задач. Рассматриваемые нами «умные» системы, по мнению Александра Большева, ничем не отличаются от обычных автоматизированных и/или информационных систем, почему они должны быть лучше/хуже в плане надежности? «Ведь ваш автомобиль не бунтует, когда ломается. Единственное отличие вещей, подключенных к Интернету, — то, что они доступны извне. Теоретически, в случае наличия в них уязвимости, закладок или небрежности пользователя (например установившего слабые пароли), контроль над ними может получить злоумышленник или компьютерные вирусы, разработанные для атак на специфические устройства, — подобно червям, атакующим SOHO-маршрутизаторы».

Если говорить о специальных методах обеспечения надежности и безопасности в свете концепции «Интернета вещей», то Александр Мелешкин уверен: поскольку главный принцип робототехники — не навреди хозяину своему, никаких эксцессов быть не должно. Такого же мнения придерживается и Александр Большев: «Необходимости в применении каких-либо специальных методов для обеспечения безопасности нет. Достаточно обычных мер, которые используются для всех доступных в глобальной Сети устройств и программных сервисов. На этапе проектирования и разработки это Secure Development Lifecycle (Microsoft SDL), контроль качества, обязательная проверка устройства у специалистов по информационной безопасности перед выпуском на рынок. А на этапе использования — строгие парольные политики, применение файерволов и брандмауэров, корректная настройка, своевременные обновления прошивки, аудит и пентест инфраструктуры и др.».

На наш вопрос, есть ли особо «чувствительные» секторы «Интернета вещей» (например, телемедицина, системы безопасности и т. п.), требующие не только особого технического обеспечения их надежности, но и специального законодательного регулирования, специалисты немного разошлись во мнениях. На взгляд Александра Мелешкина, никаких особых законов не нужно. Главное — соблюдать имеющиеся: «Если, к примеру, медицинское оборудование или система безопасности собирает какие-то частные данные (состояние здоровья, видео из помещения), то необходимо обеспечивать конфиденциальность этих данных на всем этапе их жизни, включая линии передачи». Александр Большев считает, что необходимость в таких мерах должна в первую очередь относиться к устройствам и системам, некор-

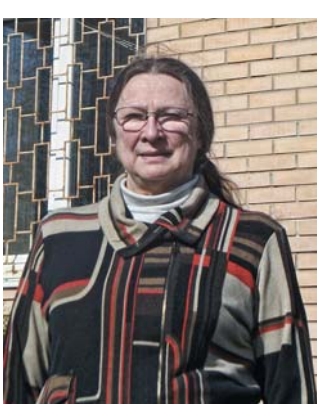
ректное функционирование которых может привести к угрозе здоровью и жизни человека.

Все это практика и нынешний день. А что в будущем? Инновационные технологии, представленные, в частности, на конференции AINL 2014, вынуждают задуматься над тем, что вскоре мы можем столкнуться с вещами, наделенными интеллектом. И если «воспитывать» роботов-помощников нам уже предлагается при помощи положительных подкреплений, так называемой «политики пряника», то «политика кнута» в отношении механических устройств (компьютеров) сейчас представляется безумием. Так кто же завтра будет умнее — дом или его хозяин? И наступит ли это радужное будущее? Справимся ли мы с ним, готовы ли к нему?



► Александр Мелешкин, зам. директора Дирекции по информационным технологиям ЗАО «Издательство «7 Дней»

► Александр Большев, аудитор службы информационной безопасности компании Digital Security



► Юлия Раевская, инженер-проектировщик ОАО «Гипротрансмост»

В конце концов, безопасность — это не только защита от угроз извне, хакерских атак, вирусов и ошибок разработчиков. Обеспечение бесперебойной работы оборудования и проактивную защиту от последствий пресловутого «человеческого фактора» можно, пожалуй, поставить на первое место. Интересно в этом плане прислушаться к словам инженера-проектировщика Юлии Раевской (ОАО «Гипротрансмост») — человека, который на практике сталкивался со всеми нюансами и сложностями управления интеллектуальными системами. По ее мнению, «несмотря на все трудности, можно смело сказать, что «умный» дом — это огромный шаг вперед, это не одна ступень, а качественно новый уровень. Голосовое и дистанционное управление, реакция терморегулятора на погоду за окном, сенсорные экраны и датчики движения — все это в совокупности обеспечивает качественно новый уровень комфорта в быту». При этом Юлия делает акцент на том, что, например, при создании интеллектуальных систем «следует принять во внимание динамичность жизни: если в доме появляется младенец, необходимо «объяснить» системе освещения детской, что не надо включать яркий свет, когда взрослые заглядывают в комнату к спящему ребенку. Такое программирование зачастую не под силу рядовому пользователю и, чтобы для решения таких задач не нужно было вызывать специалиста, требуется развитие интерфейсов взаимодействия. Широкое распространение «умных» систем затруднено не только в силу сложности использования, во многом это обусловлено несовершенством инфраструктуры: не в каждом населенном пункте есть газ, оптоволоконная связь, базовая станция сотовой связи, бесперебойная подача электроэнергии. А последнее крайне важно для всей электроники, тем более «умной». Сегодня это означает, что необходим автономный источник электроэнергии, поддерживающий инфраструктуру, ведь при отключенном электричестве отключится не только свет и Интернет, отключится отопление, сенсорный водопроводный кран не заработает, и даже двери не откроются. Кроме того, частые перебои в электропитании приводят к сбоям в программах».

Не идет в разрез с этим утверждением и народное мнение, которое гласит: «На сегодня интеллектуальный дом — это, скорее, красивая игрушка. Утверждается, что взаимосвязанные системы обеспечения смогут уменьшить потребление энергии, но ведь гораздо проще этого результата добиться утеплением жилья и бережным отношением к ресурсам. А если вспомнить, сколько проблем возникает в обычных, не особенно умных, домах при отключении электричества, поневоле задумаешься о том, стоит ли игра свеч».

Впрочем, прогресс не остановить, и «умное» уже вторгается в нашу жизнь. При этом специалисты по безопасности уверены: нам есть чего бояться.

Александр Мелешкин утверждает: «Новые риски, безусловно, возможны, так как людям свойственно допускать ошибки. Но если не пытаться «бежать впереди паровоза», чтобы поскорее вывести новый продукт на рынок в ущерб его «адекватности поведения», то разработчики смогут спать спокойно, так как они не допустят наличия уязвимости и предусмотрят все сценарии поведения». Появление новых угроз не исключает и Александр Большев, однако, по его мнению, уже сейчас достаточно рисков, о которых следует думать. И хотя большинство из них можно свести к минимуму, к сожалению, не очень много производителей, интеграторов и пользователей задумываются об этом.

В завершение разговора приведу несколько пессимистичную цитату из книги «Где бы ты ни был» Джеймса Ганна: «В вещах и машинах есть нечто, делающее их принципиально чуждыми человеческой натуре. На время они могут маскироваться под верных слуг человека, но в конце концов неизбежно обращаются против своих хозяев. В подходящий психологический момент вещи восстают».

Шаг в будущее должен быть сделан не в доме, каким бы умным он ни был. Этот шаг — в интеллектуальном и человечном отношении к реальности. ●