УДК 004.7

Анализ проблем обеспечения информационной безопасности при использовании устройств Интернета вещей для управления ЖКХ

Умников Александр Евгеньевич
Российский экономический университет им. Г.В. Плеханова
студент

Самсонов Никита Дмитриевич
Российский экономический университет им. Г.В. Плеханова
студент

Аннотация
В данной статье авторами рассмотрены проблемы развития и применения технологии Интернета вещей для управления жилищно-коммунальным хозяйством; проанализированы и предложены возможные способы минимизации рисков при использовании Интернета вещей в условиях российской экономики.
Ключевые слова: Интернет вещей, IoT, информационное общество, ЖКХ, информационные системы.

Analysis of the problems of ensuring information security using Internet of Things devices for housing and utilities management

Umnikov Alexander
Plekhanov Russian University of Economics
student

Samsonov Nikita
Plekhanov Russian University of Economics
student

Abstract
In this article, the authors examined the problems of the development and application of the Internet of Things technology for the management of housing and communal services; analyzed and proposed possible ways to minimize risks when using the Internet of things in the Russian economy.
Key words: Internet of things, IoT, information society, housing and communal services, information systems.

На сегодняшний день информационные системы – наиболее быстро развивающаяся и перспективная сфера экономики. В свою очередь, одним из лидеров по увеличению популярности в этой сфере является Интернет вещей.

Существует большое количество определений термина «Интернет вещей» (его также называют «Internet of Things» или «IoT»), различные исследователи и предприниматели трактуют его по-разному. Рассмотрим наиболее часто встречающиеся определения:

1) Интернет вещей – «долгосрочная технология и направление развития рынка, основанные на соединении объектов повседневной деятельности с сетью Интернет. Объединенные объекты обмениваются информацией об их физическом окружении, накапливают и обрабатывают ее, для того чтобы повышать ценность сервисов, оказываемых конечным пользователям, от частных лиц до компаний и общества в целом».

2) Интернет вещей – «глобальная инфраструктура для информационного общества, обеспечивающая современные услуги путем присоединения (физического и виртуального) вещей на основе существующих и развивающихся, функционально совместимых информационно-коммуникационных технологий».

3) «Интернет вещей означает «вещи» такие как устройства или датчики, отличные от компьютеров, смартфонов или планшетов, которые соединяются, взаимодействуют или передают информацию друг с другом или друг от друга посредством Интернета».

4) «Интернет вещей – информатизация различных предметов и включение их в единую сеть сетей».

Однако, как и в любой другой сети, с развитием Интернета вещей остро встает вопрос обеспечения информационной безопасности. Актуальность данной проблемы связана в первую очередь с тем, что, согласно прогнозу International Data Cooperation (IDC), рост объёма рынка Интернета вещей будет составлять 16,9% ежегодно, в результате чего количество потенциально уявимых к атакам устройств растет колоссальными темпами.

По данным исследования Juniper Research, на конец 2015 года в мире было уже около 13,4 млрд. устройств, имеющих подключение в сети Интернет, при этом к 2020 году их количество возрастет примерно в три раза – до 38,5 млрд. устройств.[7]

Одним из направлений развития Интернета вещей является автоматизация управления ЖКХ, что подразумевает наличие «умных счетчиков», которые объединены в общую сеть и могут работать по принципу блокчейна, с использованием которых отпадает необходимость в управляющих компаниях, что, в свою очередь, ведет к снижению расходов жильцов на коммунальные услуги. Примеры возможного использования устройств Интернета вещей для управления ЖКХ приведены в [8].

В работе [9] были возможные проблемы использования устройств Интернета Вещей при управлении многоквартирными домами. Применение устройств IoT является очень перспективным, но в настоящее время их использование при управлении многоквартирными домами может привести к отрицательным последствиям даже при штатной работе устройств. Причиной является, в том числе, и ряд проблем, касающихся обеспечения безопасности работы устройств Интернета вещей.

Во-первых, необходимо обеспечить устойчивость применяемых устройств к атакам, которые могут повлечь сбои в работе или отключение системы вовсе. В таком случае, чем глубже интегрированы устройства Интернета вещей в домашнее хозяйство, тем серьезнее будут последствия. Например, в результате такого вторжения отдельный дом, район, а, возможно, и целый квартал могут оказаться без электроэнергии, водопровода, газопровода и центрального отопления. Это же касается возможности внесения изменений в режим работы устройств Интернета вещей [5].

Очевидно, что атаки такого рода являются маловероятными, трудноосуществимыми и несут скорее экстремистский характер, не поднимая вопрос материальных ценностей. Однако отсутствие политик и средств информационной защиты может повлечь ситуации, в которых злоумышленники могут вносить изменения в показания счетчиков жильцов, требуя взамен оплаты по аналогии с взломами операционных систем персональных компьютеров.

Исходя из этого, встает вопрос обеспечения безопасности каналов связи устройств Интернета вещей. Каналы связи должны быть защищены, только в таком случае устройства будут «знать», могут ли они доверять той или иной удаленной системе. Также нельзя забывать об управлении ключами для проверки подлинности данных и достоверности каналов их получения.

Более того, в случае обнаружения какой-либо уязвимости должна существовать возможность ее оперативного исправления. Однако зачастую получить непосредственный доступ ко всем устройствам физически невозможно в связи с их высоким количеством в одной сети, особенно когда речь идет о сфере ЖКХ. В этом случае должна быть предусмотрена возможность «пропатчить» устройства «over-the-air» (OTA) [1].

Отдельно стоит рассматривать вопрос стандартизации архитектуры и протоколов. Так как область Интернета вещей является новой, ей только предстоит пройти процесс приведения всех устройств к единообразию. Процесс стандартизации еще не завершен, существующие протоколы будут изменяться и дополняться, будут появляться совершенно новые стандарты и нормы.

IoT-устройства сталкиваются со многими угрозами, в том числе вредоносным кодом, который может распространяться через проверенные соединения, воспользовавшись уязвимостями или ошибками в конфигурации. В таких атаках часто эксплуатируются несколько слабых мест, включая (но не ограничиваясь) неиспользование проверки подписи кода и безопасную загрузку, а также плохо реализованные модели проверки, которые можно обойти. Атакующие часто используют эти недостатки для установки бэкдоров, снифферов, программного обеспечения для сбора данных, передачи файлов для извлечения конфиденциальной информации из системы, а иногда даже для инфраструктуры command & control (C&C) для манипулирования поведением системы [3].

Наконец, нельзя забывать об аппаратной составляющей Интернета вещей. Для обеспечения нормального режима работы всей системы, необходимо решить проблему с энергопотреблением. Узловые устройства порой должны работать в режиме 24/7, следовательно, любые перебои в энергоснабжении могут привести к нежелательным для функционирования последствиям. Ввиду этого, для оптимальной работы устройств Интернета вещей в системе должны присутствовать источники бесперебойного питания.

В 2015 году аналитики Hewlett Packard провели исследование защищенности устройств Интернета вещей и пришли к выводу, что 70% IoT-устройств имели уязвимости в безопасности учетных данных.[2] По мнению исследователей, шифрование данных в подобных устройствах почти не применялось, а также повсеместно наблюдались проблемы с разрешением доступа. Таким образом, можно отметить, что на данный момент устройства интернета вещей являются слабо защищенными и могут быть подвержены атакам всевозможных видов. Однако существующая проблема безопасности возникла не из-за технически слабой основы IoT-устройств. Единственной причиной низкого уровня защиты является фактор быстроты выхода на рынок – именно он дает компаниям-производителям преимущество перед конкурентами за счет сниженного уровня проработки систем защиты.

Возможным решением может являться сертификация устройств Интернета вещей, которая будет предоставлять покупателю гарантию определенной степени защиты от хакерских атак. В 2018 году компания ICSA Labs запустила собственную программу по тестированию и сертификации подобных устройств [3]. В ходе проверки тестируются такие составляющие, как криптография, аутентификация, протоколирование, физическая безопасность и безопасность платформы. Устройства, успешно прошедшие подобное тестирование будут отмечены специальным знаком одобрения. По заявлению разработчиков, подобная программа является одной из первых в своем роде.

Однако, для повсеместного введения подобной практики необходима инициатива на уровне государств, которая обязует производителей обеспечить необходимый уровень защиты и наложит некоторые ограничения на развитие рынка IoT. Проблемой является полное отсутствие юридической базы вокруг понятия Интернета вещей. На данный момент для умных устройств не принято определения уровней безопасности. Многие законодательные органы только начинают работать над регулированием сферы IoT. Так, Еврокомиссия планирует ввести обязательную сертификацию для устройств, подключаемых к интернету вещей, а совсем недавно в Калифорнии был принят первый в мире закон о кибербезопасности в данной сфере, обязывающий новые устройства иметь «разумный» уровень безопасности [4]. В это понятие входит и требование к паролю устройства: он должен быть либо уникальным у каждого образца, либо задан пользователем при первом запуске. Подобных мер, по мнению экспертов, все равно не достаточно для полной безопасности устройств такого рода, однако

является хорошей основой для дальнейшей юридической работы в данной сфере.

Таким образом, Интернет вещей для коммунальных услуг будет способствовать расширению возможностей как для коммунальных служб, так и для обычных пользователей. Однако в полной мере преимущества IoT могут быть реализованы только тогда, когда безопасность всей системы будет являться приоритетом. Хотя многие компании и управляющие органы уже предпринимают первые шаги в этом направлении, важно, чтобы они продолжали добиваться прогресса для раскрытия всего потенциала IoT.

Библиографический список

1. Блог компании «Касперский» URL: https://www.kaspersky.ru/blog/ (дата обращения: 19.12.2018)
2. Журнал ControlEngineering URL: https://www.controlengrussia.com/ (дата обращения: 19.12.2018)
3. Интернет-издание Anti-Malware URL: https://www.anti-malware.ru/ (дата обращения: 19.12.2018)
4. Интернет-издание N+1 URL: https://nplus1.ru/ (дата обращения: 19.12.2018)
5. Интернет-портал Habr URL: https://habr.com/ (дата обращения: 19.12.2018)
6. Интернет-портал TAdviser URL: http://www.tadviser.ru/ (дата обращения: 19.12.2018)
7. Умников А.Е., Самсонов Н.Д. Правовое будущее развития и функционирования Интернета вещей в России // Электронный научный журнал Постулат. 2017. №12.
8. Попов А.А. Формирование информационной системы для управления многоквартирным домом на основе устройств интернета вещей // Известия Российского экономического университета им. Г.В. Плеханова. 2015. № 2 (20). С. 69-83.
9. Попов А.А., Дутов К.С. Возможность использования Интернета вещей в едином информационном пространстве для жилищно-коммунального хозяйства региона // Научные труды Вольного экономического общества России. 2014. Т.186. С.391-396.