УДК 004

Проблемы информационной безопасности при использовании технологии Интернет вещей для городской среды

Озерова Елизавета Алексеевна
Российский экономический университет им. Плеханова
студент

Соколова Марина Александровна
Российский экономический университет им. Плеханова
студент

Аннотация
В статье представлено краткое описание основных проблем информационной безопасности, возникающих на каждом уровне работы системы, в таких развивающихся технологиях как «Интернет вещей» в целом и «Умный город» в конкретике. Рассмотрены существующие решения по защите информации, а также предложены новые возможные варианты.
Ключевые слова: Интернет вещей, информационная безопасность, Умный город, Умный дом, защита данных

Problems of information security when using the Internet of Things technology for the urban environment

Ozerova Elizabeth Alekseevna
Plekhanov Russian University of Economics
student

Sokolova Marina Aleksandrovna
Plekhanov Russian University of Economics
student

Abstract
The article is a summary of the main information security problems, which occur at every level of the systems work cycle in such emerging technologies as the «Internet of Things» in general and «Smart City» in particular. Existing solutions for data protection are reviewed and new options are offered.
Keywords: Internet of things, information security, Smart city, Smart house, data security

Введение

В 1926 году известный изобретатель Никола Тесла в интервью для журнала «Collier's» предсказал, что уже в недалеком будущем радио будет преобразовано в «большой мозг», а все вещи станут частью единого целого

[6]. Спустя всего несколько десятков лет данная концепция действительно смогла воплотиться в жизнь и вскоре стала еще одним шагом к большому технологическому будущему. В 1999 году идея была официально сформулирована как применение средств радиочастотной идентификации для взаимодействия физических предметов между собой и с внешним окружением и получила название «Интернет вещей».

Далее последовал достаточно высокий скачок в развитии этой сети. Уже в 2008-2009 годах произошел переход от «Интернета людей» к «Интернету вещей», то есть количество подключенных к сети физических предметов превысило количество людей.

Сейчас эта сеть получила распространение почти на все стороны деятельности жизни и общества, и самого человека. Концепция на данный момент реализована уже во многих странах и известна многим, например, как «Умный дом», «Промышленный интернет вещей» и что более интересно «Умный город».Фактически, уровень внедрения достиг такой степени, что в отношении масштабных решений с применением «Интернета вещей»появился термин «Интернет всего»(Internet of Everything).

Но любое развитие несет за собой множество новых трудностей. Известный журналист Лоуренс Круз как-то сказал: «Сначала, как водится, хорошая новость: «Интернет вещей» существует, неся нам огромные удобства, удовольствия и преимущества. А теперь – плохая новость: «Интернет вещей» создает серьезные проблемы для информационной безопасности» [3].

В работе [1] были рассмотрены проблемы использования устройств Интернета Вещей применительно к управлению многоквартирными домами. Отмечается, что, несмотря на перспективность применения устройств IoT, их использование в настоящее время для управления многоквартирными домами может привести к нежелательным и неожиданным отрицательным последствиям (в том числе, вследствие больших проблем с информационной безопасностью).

Особого внимания заслуживает именно тематика «Умного города». В разных странах реализуются проекты по строительству новых «умных» кварталов или целых населенных пунктов, а также по модернизации существующих городов. По всему миру насчитывается более 140 проектов «Умных городов» разной степени завершенности и это далеко не предел [7]. Однако одной из главных причин сложного развития данной концепции заключается именно в невозможности предоставления полной информационной безопасности в «Умных городах».

Действительно, с новшествами в ИТ сфере появляются новые требования по защите информации. «Интернет вещей» начался с формирования самой структуры и работы системы, поэтому проблема информационной безопасности еще не развита и не закрыта. Чем сильнее программные приложения будут проникать в повседневную жизнь, тем опасней будут угрозы. В отчете Всемирного экономического форума говорится, что выработка единого подхода к решению проблемы

безопасности – самый необходимый шаг для развития «Интернета вещей» и всех входящих в него концепций, таких как «Умный город».

Информационные системы на основе Интернета Вещей пока что не сформировались как единое целое. Пока что существуют лишь разрозненные и практически не связанные между собой сети устройств IoT, которые предназначены для решения каких-либо специфических задач (например, «умные» транспортные, парковочные службы, служба контроля улиц и придомовых территорий). По мере совершенствования технологий IoTтакие сети могут быть соединены друг с другом, и тогда можно будет утверждать о появлении информационных систем и информационных сервисов на основе IoT. Предполагается, что такие информационные системы и сервисы будут представлять собой совокупность четырех контуров: информационного, сенсорного, пользовательского и управленческого [2].

В России уже существуют проекты по реализации идеи «Умный город». К примеру, «Умный» и безопасный город Казань», подразумевающий создание единой городской инфраструктуры, которая сможет осуществить предоставление жителям города, компаниям и госучреждениям различные общественные услуги («Безопасный город», «Умное» уличное освещение», «Умное» ЖКХ» и др.).

Однако с каждым новым проектом вопрос о безопасности данных становится все более и более значительным. Если концепция «Умный дом» способна подвергнуть угрозе со стороны злоумышленников конкретную группу лиц, то проекты «Умного города» могут нанести ущерб немалой части населения. Именно поэтому проблемы информационной безопасности в тематике «Интернет вещей» сейчас очень актуальны и требуют подробного исследования в целях нахождения всевозможных путей их решений.

Постановка проблемы исследования

В процессе разработки вопрос о безопасности информации в работе подобных концепций, безусловно, встает на первое место. Беспроводная технология для связи между отдельными устройствами, в руках злоумышленников действительно способна нанести огромный ущерб. Именно поэтому без надлежащей защиты данных ни один из потенциальных пользователей не будет осуществлять эксплуатацию данной сети.

Угрозы информационной безопасности можно разделить на определённые типы. Во-первых, это угрозы конфиденциальности – случай несанкционированного доступа к данным, угрозы целостности данных, а также угрозы доступности – ограничение или блокирование доступа к данным (например, DDoS-атаки) [5].

Проблема информационной безопасности сети «Интернет вещей» и ее концепций имеет разноуровневую структуру. В основном принято выделять: уровень восприятия, сетевой, а также прикладной уровни. На каждом этапе осуществление защиты данных имеет свои трудности и значение, поэтому необходимо рассматривать каждый уровень в отдельности.

Информационная безопасность на уровне восприятия имеет высокое значение, поскольку именно здесь происходит предоставление информации. На данном уровне возникают такие проблемы защиты данных, как физический захват сенсорных узлов, захват узла шлюза, истощение энергообеспечения, опасность маршрутизации установлением в сеть нелегитимных сенсоров и копирования узла. Также существуют угрозы целостности данных, под которыми подразумевается нарушение целостности данных в случаях удаления лишних элементов, добавления, а также изменения в порядке расположения данных. Не менее важная проблема – это атаки типа DoS - случай, когда вследствие атаки злоумышленников доступ к предоставляемым системным ресурсам ограничен, либо полностью отсутствует [8].

Защита данных на сетевом уровне полностью связана с осуществлением безопасности непосредственно самой сети. Здесь тоже поднимается вопрос о целостности данных, а также об их перехвате, конфиденциальности и другом. Возможны межсетевые проблемы аутентификации, по причинам различных атак как типа DDos, DoS, так и атаки посредника. На данном этапе злоумышленники могут также нарушить структуру программ посредством их заражения вредоносным программным обеспечением. Ко всему прочему, более опасными угрозами являются проблемы масштабируемости сети, которые возникают в случае заранее не предсказуемого объема передачи данных от большого числа узлов.

Важной проблемой нарушения информационной безопасности является уязвимость программного обеспечения. В случае ошибок непосредственно в разработке самого ПО, его внедрения, обработки не всех возможных исключений, ошибок в базах данных, недостаточной производительности и многого другого защита информации не способна выполнить свое назначение и система подвергается внешнему вмешательству. Почему же так сложно организовать разработку правильно структурированного, безопасного программного обеспечения? Проблема заключается в огромном разнообразии используемых аппаратных платформ и операционных систем. При проектировании программного обеспечения применяется эмуляция поведения приборов «Интернета вещей» с условием наибольшего соответствия поведению оригинальной системы. Поскольку каждый прибор обладает своими ограничениями, такими как энергообеспечение, производительность процессора, память и многое другое, происходит значительное расхождение между эмуляторами и приборами, что приводит к неверно спроектированному ПО.

Прикладной уровень обеспечивает взаимодействие пользовательских приложений с сетью. Во-первых, здесь нарушение защиты данных возникает по причине угроз искажения, повтора, раскрытия информации и многого другого. Во-вторых, приложения Интернет вещей сталкиваются с дополнительными проблемами безопасности. Например, во время использования облачных вычислений, при обработке информации, при защите приватности и др. [8].

Вопрос о том, на каком именно этапе безопасность информации подвергается наибольшему риску, рассматривается многими исследователями. На данный момент не существует единого мнения по данной проблеме, поскольку абсолютно на каждом уровне разработчики сталкиваются с определенными угрозами, которые требуется заранее предусмотреть и предотвратить.

Обзор существующих путей решения проблемы

Джефф Кац (Jeff Katz) выступивший на конференции PHDays безопасности «Интернета вещей» в своем докладе произнес такую фразу: «Нельзя сказать, что устройство на сто процентов безопасное. Мы можем говорить, что это устройство, кажется, безопасно или что оно точно не безопасно». Таким образом, приборов, полностью обеспечивающих безопасность, не существует: либо определенные недостатки в защите были обнаружены, либо пока нет, но в скором времени их найдут.

По многим данным почти каждый производитель, предоставляющий услуги и товары рынка «Интернет вещей», нарушает принцип сквозной информационной безопасности, рекомендованный к применению для всех услуг и продуктов информационно-коммуникационных технологий. Опираясь на этот принцип, информационную безопасность необходимо разрабатывать уже на первых этапах проектирования продукта или услуги и поддерживать до самых последних стадий их жизненного цикла. Данную проблему, возможно, решить только лишь на законодательном уровне, путем создания новых законов, которые будут обязывать поставщиков следовать подобному принципу.

Не менее важным решением проблем, связанных с информационной безопасностью сети «Интернет вещей», является создание стандартов по этой категории. Наличие достаточно небольшого количества стандартов напрямую сказывается на проектировании, как самих устройств, так и программного обеспечения. По мнению многих экспертов, выработать единый общий стандарт, как для «Интернета вещей», так и конкретно для «Умного города» окажется невозможным, вместо этого, скорее всего, уже через несколько лет появится небольшой набор стандартов, основанных на практическом передовом опыте [3]. Международная группа стандартов ISO уже сформировала рабочую группу, которой предстоит разрабатывать адаптацию семейства стандартов безопасности ISO 27000 к применению их в сфере «Интернета вещей» [4].

За последние годы было создано несколько отраслевых союзов производителей «Интернета вещей», например, таких как: Thread Group, Open Interconnect Consortium, All Seen Alliance и Industrial Internet Consortium [4]. Не смотря на то, что каждая группа осуществляет работу в своей сфере, опираясь на интересы своих пользователей, каждый из них поддерживает идею расширения практики шифрования данных и использования других способов защиты.

Решением поставленной проблемы также может оказаться расширение сектора, включающего компании в сфере разработки «Интернета вещей», которые уже сейчас занимаются проектированием возможных путей предотвращения угроз информационной безопасности в этой области. На данный момент ведущие технологические корпорации пока не проводят активные работы по обеспечению безопасности сети, поэтому данная обязанность лежит на множестве стартап-компаний, в большей степени обеспечивающих нынешний рост сектора «Интернета вещей». Консалтинговая компания Gartner сделала прогноз, что к 2017 году большая часть продуктов «Интернет вещей» будет производиться небольшими компаниями, которые существуют не более трех лет [4]. Естественно, лишь малая часть этих компаний будет способна обеспечить подходящий уровень безопасности своих продуктов. Именно поэтому очень важно, чтобы уже сейчас на рынок данного сектора вступили гиганты индустрии – корпорации, которые смогут выделить средства на открытие проектов по обеспечению информационной безопасности сети «Интернет вещей».

Заключение

Таким образом, исследование ряда проблем информационной безопасности «Интернета вещей» и вытекающей из нее концепции «Умного города» позволило выявить всевозможные пути решений. Также исследование показало, насколько важна на данный момент поднятая тематика и насколько значительна проблема недостаточной вовлеченности крупных организационных структур в этой сфере.

Создание «умных» городов уже стало важным трендом мирового развития. Внедрение «Умного города» способствует повышению качества жизни граждан, а также развитию городского хозяйства. Как отмечает Сандир Агарвал, руководитель инженерного подразделения компании Happiest Minds Technologies, возведение «умного» города предусматривает решение ряда базовых задач, таких как: построение «умной» экономики, воспитание «умного» потребителя, создание «умной» муниципальной системы управления и многое другое [9].

Естественно, важным аспектом является обеспечение безопасности данных в каждой из ряда систем. Необходимо защищать централизованные базы данных, ресурсы и сервисы, отвечающие за бесперебойную и корректную работу систем городской инфраструктуры, ресурсы, представляющие государственные услуги гражданам, и другие составляющие «умного» города [9]. Только соблюдая определенные принципы и следуя необходимым стандартам, возможно, построить безопасную инфраструктуру на основе концепции «Умного города», позволяющую в значительной степени улучшить жизнь общества по многим показателям.

Библиографический список

1. 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
2. Попов А.А. Разработка облачного информационного сервиса дляфункционирования инновационной ИТ-инфраструктуры организации по управлению многоквартирными домами // Известия Российского экономического университета им. Г.В. Плеханова. 2013. №4(14). С.19-57
3. «Интернет вещей и информационная безопасность»Сайт. - URL: http://club.cnews.ru/blogs/entry/internet_veshchej_i_informatsionnaya_bezopasnost
4. «Как обезопасить интернет вещей?» Сайт. - URL: http://rb.ru/story/IoT-security/
5. Галяутдинов Р.Р. «Информационная безопасность. Виды угроз и защита информации» Сайт. URL: http://galyautdinov.ru/post/informacionnaya-bezopasnost
6. «Тайны Будущего. Никола Тесла: «Земля превратится в огромный мозг...» Сайт. URL: http://nnm.me/blogs/spravedliviy/tayny-budushego-nikola-tesla-zemlya-prevratitsya-v-ogromnyy-mozg/
7. «Умные» города. Перспективы развития в России». Сайт. URL: https://www.iemag.ru/analitics/detail.php?ID=34007
8. «Проблемы безопасности Интернет вещей: обзор». Научная библиотека КиберЛенинка. Сайт. URL: http://cyberleninka.ru/article/n/problemy-bezopasnosti-internet-veschey-obzor#ixzz4MmVVn6W0
9. «Интернет вещей и «умные» города: рекомендации экспертов» Сайт. URL:https://www.pcweek.ru/iot/article/detail.php?ID=186989