Угрозы безопасности узкополосного Интернета Вещей и меры противодействия

А.У. Менциев[1], *Х.Х. Пахаев*[1], *Т.Г. Айгумов*[2]

[1] *ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова»*

[2] *ФГБОУ ВО «Дагестанский государственный технический университет»*

Аннотация: Технологии Интернета вещей стали неотъемлемой частью деловой и общественной жизни. Эту технологию можно увидеть практически в каждом крупном городе России. Многие ведущие страны находятся на относительно высоком уровне массового внедрения технологии Интернета вещей. Многие направления деятельности страны напрямую зависят от Интернета вещей: «умный дом», «умный город», цифровое сельское хозяйство, автоматизация производства и др. При этом необходимо учитывать, что разностороннее использование технологий влечет за собой особый интерес злоумышленников и рост угроз безопасности. В связи с этим у специалистов возникает вопрос обеспечения безопасности. В этой статье обсуждаются характеристики устройств Интернета вещей, основные угрозы безопасности узкополосного Интернета вещей и рекомендации по контрмерам.

Ключевые слова: Интернет вещей, NB-IoT, кибербезопасность, угрозы безопасности, компьютерная безопасность.

Интернет вещей (IoT) - одно из самых крупных и быстрорастущих изобретений последнего десятилетия, и рост в этой отрасли можно оценить по огромному количеству устройств, подключенных к сети «Интернет вещей». В развитых странах устройства, подключенные к Интернету вещей, во многом стали частью повседневной жизни. К концу 2019 года количество этих устройств, подключенных к сети IoT, превысило 26,66 миллиарда и продолжает расти, поскольку каждую секунду во всем мире к Интернету подключаются 127 новых устройств [1].

Что означает это постоянно увеличивающееся количество устройств? Чем больше устройств подключено к сети IoT, тем более уязвимой она становится для различных угроз и рисков безопасности. Многие устройства Интернета вещей, подключенные к Интернету, обрабатывают данные чрезвычайно конфиденциального характера, доступ к которым должен иметь только уполномоченный персонал. Эти приложения представляют собой

компьютерные программы, которые большую часть времени используют условия реального времени для обеспечения успешного выполнения задач.

Одна из причин уязвимости к рискам безопасности заключается в том, что производители устройств, подключаемых к сетям IoT, не считают конфиденциальность или безопасность устройства и данных приоритетом. Следовательно, многие пользователи, не подозревая об этом, по-прежнему покупают эти устройства и подключают их к сети IoT, увеличивая риск нарушения безопасности и т. д. [2].

Характеристики устройств Интернета вещей

Мы собираемся обсудить некоторые характеристики устройств Интернета вещей, которые создают повышенную угрозу безопасности. Определив характеристики, которые приводят к проблеме, можно найти решение этой проблемы. Однако даже базовое определение Интернета вещей может дать понимание, что является основной причиной угроз безопасности.

Интернет вещей – это совокупность миллиардов устройств по всему миру, подключенных друг к другу через Интернет. Мало того, эти IoT-устройства также подключены к облаку через всемирную сеть для обмена данными с другими IoT-устройствами и, таким образом, становятся уязвимыми для хакеров по всему миру. Некоторые основные характеристики устройств IoT включают в себя:

- Сбор данных в реальном времени для выполнения своих задач,
- Постоянное использование сотовой сети LPWAN, которую также называют Narrowband IoT и LTE-M,
- Измерение физических параметров и способность выполнять физические действия,
- Перманентное подключение к облаку,
- Умение принимать решения самостоятельно на основе имеющихся данных [3].

Угрозы безопасности узкополосного Интернета вещей

Обсуждаемые выше характеристики дают нам представление о проблемах, с которыми сталкивается узкополосный Интернет вещей. Теперь мы собираемся обсудить эти многочисленные проблемы и причину, по которой многие устройства Интернета вещей сталкиваются с проблемами. Одно из самых больших недоразумений на рынке, связанных с безопасностью IoT, заключается в том, что само понятие безопасности означает только повышение безопасности устройств IoT, в то время как требуется гораздо больше [4]. Когда мы говорим: «Интернет вещей», мы имеем в виду полную систему, а не только устройства повседневного использования. Эта система включает в себя само устройство, облако, мобильное приложение, которое используется для управления устройством, сетевой интерфейс, к которому подключено устройство, и программное обеспечение; помимо этого – работа в системе, использование шифрования, аутентификации и, наконец, физическая безопасность как устройства, так и всех других физических компонентов. Таким образом, наряду с устройством IoT, все эти компоненты системы в равной степени уязвимы для угроз и проблем безопасности, которые мы собираемся обсудить [5]. Давайте теперь углубимся в эти проблемы одну за другой.

А. Плохая безопасность приложений и конечных точек

Как гласит английская фраза: «Цепь настолько сильна, насколько сильно ее самое слабое звено». Случай с системами IoT очень похож. Независимо от того, насколько хороша общая безопасность, если вы используете устройство с плохой безопасностью, вся система может быть легко взломана [5]. То же самое касается безопасности приложений. Плохо защищенные приложения и конечные устройства делают системы уязвимыми для кибератак. Одна из основных причин заключается в том, что большинство производителей устройств – это те же производители, которые

производили устройства до появления IoT, а теперь они сделали свои устройства умными, чтобы подключаться к IoT, но не учли вопросы безопасности, потому что для них это несущественная функция. Аналогично обстоит дело с разработчиками приложений. Однако безопасность является важной особенностью устройства или приложения в системе IoT [6].

Б. Лёгкая авторизация / аутентификация

Как обсуждалось ранее, все устройства IoT требуют определенной формы авторизации или аутентификации, чтобы обезопасить их от кражи данных или других угроз безопасности. Но даже по сей день большинство устройств, выпускаемых на коммерческом рынке, поставляются с процессорами настолько маленькими, что они предназначены только для выполнения очень простых задач и не могут обрабатывать что-то вроде авторизации или аутентификации, для которых требуется процессор большего размера. Вы можете задуматься, сколько вычислительной мощности может потребоваться для такой простой задачи, как аутентификация, но вы ошибаетесь, если полагаете, что большинство коммерческих устройств вообще способны на это [7].

В. Отсутствие физической безопасности

Вся идея Интернета вещей заключается в создании современных и умных городов, в которых каждое устройство каждого дома взаимодействует и обменивается данными с системой, чтобы разумно управлять системой. Это означает, что большинство устройств Интернета вещей находятся в городских условиях и доступны для общественности. Более того, городская инфраструктура иногда может быть очень сложной и плотной до такой степени, что невозможно обеспечить физическую безопасность системы. Это увеличивает риск физической атаки. Мы не имеем в виду, что какой-то преступник может повредить систему в буквальном смысле, но хакеры могут

легко получить доступ к системе IoT, которая находится в открытом доступе, с целью кражи данных и нарушения работы устройств [8].

Г. Чрезмерное количество конфиденциальных данных

Интеллектуальное устройство – это устройство, которое имеет некоторые базовые встроенные функции, такие, как микрофон, камера, ночное видение и т.д., которые необходимы для приема, передачи данных и взаимодействия с пользователем. Эти функции действуют как глаза и уши устройства и непрерывно записывают терабайты данных, иногда без ведома пользователя, использующего данные устройства. Такие данные могут быть очень конфиденциальными, и, если попадут в чужие руки, могут нарушить конфиденциальность пользователя и стать серьезной угрозой безопасности. Это одна из основных причин того, что люди не могут доверять системам Интернета вещей, и были сотни сообщений о случаях, когда сборщики данных злоупотребляли информацией и нарушали многие законы о конфиденциальности данных [9].

Д. Небезопасные учетные данные по умолчанию

Когда вы покупаете новое устройство IoT или любое другое устройство, оно обычно поставляется с именем пользователя по умолчанию и паролем по умолчанию, который вы используете для первого входа в систему на устройстве. Это имя пользователя и пароль по умолчанию называются учетными данными по умолчанию и могут представлять огромную угрозу безопасности. Некоторые из устройств IoT даже по сей день поставляются с жестко запрограммированными паролями и именами пользователей, что означает, что эти учетные данные никогда не могут быть изменены и иногда отпечатываются на устройстве. Это делает устройство уязвимым не только для кибератак, но и для физических атак, когда кто-то может получить доступ к имени пользователя или паролю по умолчанию. Некоторые пользователи вовсе не меняют этих учетных данных, что делает их устройства ещё менее

безопасными. Хакеры всегда пытаются получить доступ к устройствам, используя имя пользователя и пароль по умолчанию [10].

Контрмеры угроз безопасности узкополосного Интернета Вещей

Существует ряд контрмер, которые можно предпринять для обеспечения безопасности систем Интернета Вещей. Эти контрмеры включают в себя участие всех, от пользователя до производителей и разработчиков приложений и т. д. Вот некоторые из шагов, которые каждый из нас должен выполнить, прежде чем переключиться на интеллектуальные устройства, подключенные к Интернету Вещей.

Первый и самый важный шаг, который необходимо сделать производителям и разработчикам приложений, – это осознать важность безопасности в устройствах IoT и начать рассматривать ее как приоритет, а не функцию. Все новые производимые устройства Интернета Вещей и все разрабатываемые приложения Интернета Вещей должны быть защищены от начала до конца и не допускать утечки данных. Как пользователь, мы можем сделать для обеспечения безопасности приложений и конечной точки следующее: при покупке устройств или установке приложения мы должны убедиться, что оно от надежного производителя или разработчика. Большинство брендов на рынке надежны с точки зрения безопасности, проблема возникает только тогда, когда производители с местных рынков пытаются продвинуть свой продукт, не уделяя внимания безопасности [11].

Второй наиболее важный шаг, который необходимо предпринять, - это необходимость аутентификации и авторизации при использовании интеллектуальных устройств, подключенных к Интернету Вещей. Производители и разработчики должны убедиться, что их устройства и приложения поддерживают безопасную авторизацию и аутентификацию. Пользователи также должны убедиться, что устройство, которое они покупают, имеет эту встроенную функцию. Для устройств, которые уже

работают, но не поддерживают даже базовые функции, такие, как аутентификация и авторизация, могут использоваться вторичные приложения и устройства, которые обеспечивают дополнительную безопасность в форме аутентификации или авторизации. Пользователь также должен убедиться, что он не приобретает устройства с жестко заданными учетными данными по умолчанию, чтобы сразу при получении устройства сменить логины и пароли.

С точки зрения данных, пользовательские данные являются одним из основных компонентов, которые увеличивают риск и должны передаваться безопасным способом. Сборщики данных и поставщики должны сделать безопасность данных своим главным приоритетом и обеспечить безопасную передачу данных с одного устройства на другое. Правительства по всему миру должны сыграть огромную роль на этом этапе, и им следует убедиться, что поставщики данных, разработчики приложений и т. д. не злоупотребляют пользовательскими данными. Необходимо разработать специальные законы и постановления, чтобы помешать этим людям злоупотреблять общедоступными данными [12].

Еще один важный шаг, который необходимо предпринять, - это обеспечить наличие системы мониторинга, которая отслеживает всю систему от конечной точки устройства до сетевой безопасности. В случае эксцесса она всегда найдет самое слабое звено цепи и предпримет ответные действия, чтобы предотвратить повторение ситуации. Приложение, используемое в системах Интернета Вещей, должно иметь встроенные функции для записи отклонений в данных и последующего сообщения об этом, чтобы пользователь мог принять соответствующие меры.

И последнее, но не менее важное: необходимо создать многоуровневую систему для защиты системы Интернета Вещей, которая сама по себе является сложной взаимосвязанной системой. Эти многочисленные уровни

должны включать административные, технические и физические средства контроля, которые всегда существуют для защиты сети Интернета Вещей от любых неблагоприятных факторов и всегда готовы принять меры. Без достаточного уровня безопасности и защиты данных Интернет вещей не может и не будет оставаться успешным в долгосрочной перспективе и неизбежно потерпит неудачу. Поэтому руководство, производители, разработчики и сами пользователи должны сделать безопасность приоритетом номер один при работе с устройствами, подключенными к Интернету Вещей.

Литература

1. Maayan G.D. The IoT Rundown For 2020: Stats, Risks, and Solutions. Security Today. 2020. pp. 1-4. URL: securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx

2. Malan J., Eager J., Lale-Demoz E., Ranghieri C.G. and Brady M. Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape. Centre for Strategy & Evaluation Services LLP. 2020. pp. 1-102.

3. Ugwuanyi S., Paul G. and Irvine J. Survey of IoT for Developing Countries: Performance Analysis of LoRaWAN and Cellular NB-IoT Networks. Electronics. 2021, №10(2224). pp. 1-30.

4. Langkemper S. The Most Important Security Problems with IoT Devices. Eurofins Cyber Security. 2020. URL: eurofins-cybersecurity.com/news/security-problems-iot-devices/.

5. Heubl B. How to hack an IoT device. Engineering and Technology. 2019. URL: eandt.theiet.org/content/articles/2019/06/how-to-hack-an-iot-device/.

6. Gillis A.S. What is internet of things (IoT)? IoT Agenda. 2020. URL: internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

7. Tawalbeh L., Muheidat F., Tawalbeh M. and Quwaider M. IoT Privacy and Security: Challenges and Solutions. Applied Sciences. 2020. pp. 1-17.

8. Polat G. Security Issues in IoT: Challenges and Countermeasures. ISACA JOURNAL. 2019. pp. 1-7.

9. Petters J. Data Privacy Guide: Definitions, Explanations and Legislation. Varonis. 2020. URL: varonis.com/blog/data-privacy/.

10. Cynthia J., Parveen Sultana H., Saroja M. N. and Senthil J. Security Protocols for IoT. Ubiquitous Computing and Computing Security of IoT. 2019. pp. 1-28.

11. Халиев С.У., Пахаев Х.Х. Информационная безопасность в робототехнике // Инженерный вестник Дона, 2019, №4. URL: ivdon.ru/ru/magazine/archive/n4y2019/5833

12. Леонов Д.В. Моделирование, с внедрением блока адаптивного мониторинга, системы комплексной защиты конфиденциальной информации, от кибернетических атак // Инженерный вестник Дона, 2019, №6. URL: ivdon.ru/ru/magazine/archive/N6y2019/6035

References

1. Maayan G.D. The IoT Rundown For 2020: Stats, Risks, and Solutions. Security Today. 2020. pp. 1-4. URL: securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx

2. Malan J., Eager J., Lale-Demoz E., Ranghieri C.G. and Brady M. Framing the Nature and Scale of Cyber Security Vulnerabilities within the Current Consumer Internet of Things (IoT) Landscape. Centre for Strategy & Evaluation Services LLP. 2020. pp. 1-102.

3. Ugwuanyi S., Paul G. and Irvine J. Survey of IoT for Developing Countries: Performance Analysis of LoRaWAN and Cellular NB-IoT Networks. Electronics. 2021, №10(2224). Pp. 1-30.

4. Langkemper S. The Most Important Security Problems with IoT Devices. Eurofins Cyber Security. 2020. URL: eurofins-cybersecurity.com/news/security-problems-iot-devices/.

5. Heubl B. How to hack an IoT device. Engineering and Technology. 2019. URL: eandt.theiet.org/content/articles/2019/06/how-to-hack-an-iot-device/.

6. Gillis A.S. What is internet of things (IoT)? IoT Agenda. 2020. URL: internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

7. Tawalbeh L., Muheidat F., Tawalbeh M. and Quwaider M. IoT Privacy and Security: Challenges and Solutions. Applied Sciences. 2020. pp. 1-17.

8. Polat G. Security Issues in IoT: Challenges and Countermeasures. ISACA JOURNAL. 2019. pp. 1-7.

9. Petters J. Data Privacy Guide: Definitions, Explanations and Legislation. Varonis. 2020. URL: varonis.com/blog/data-privacy/

10. Cynthia J., Parveen Sultana H., Saroja M. N. and Senthil J. Security Protocols for IoT. Ubiquitous Computing and Computing Security of IoT. 2019. pp. 1-28.

11. Khaliev M. S-U., Pakhayev Kh.Kh. Inzhenernyj vestnik Dona, 2019, №4. URL: ivdon.ru/ru/magazine/archive/n4y2019/5833

12. Leonov D.V. Inzhenernyj vestnik Dona, 2019, №6. URL: ivdon.ru/ru/magazine/archive/N6y2019/6035