УДК 004.031.4
О.В.Іванчук, В.М.Козел, Є.А. Дроздова
Херсонський національний технічний університет
E-mail: k_vic@ukr.net

ДОСЛІДЖЕННЯ СИСТЕМ ЗБОРУ ІНФОРМАЦІЇ ВІД IoT ПРИСТРОЇВ

У статті розглянуті проблеми поширення IoT-пристроїв. Виявлені проблеми, які заважають широкому розповсюдженню і застосуванню IoT-пристроїв. Виконано огляд системи Orvibo Zigbee Minihub EU і зроблено висновок, що система не дозволяє здійснювати збір даних з будь-яких IoT-пристроїв. Orvibo Zigbee Minihub EU дозволяє використання тільки пристроїв за допомогою власного протоколу Zigbee. Розроблена програмна реалізація збору інформації від IoT-пристроїв з подальшою можливістю аналізувати і обробляти отримані дані і виконувати запити від даних пристроїв.

Ключові слова: інтернет, інтернет речей, IoT платформа, мережа пристроїв, розумний будинок, комп'ютерна система, безпека, програмне забезпечення.

А.В. Иванчук, В.Н. Козел, Е.А. Дроздова
Херсонский национальный технический университет
E-mail: k_vic@ukr.net

ИССЛЕДОВАНИЕ СИСТЕМ СБОРА ИНФОРМАЦИИ ОТ IoT УСТРОЙСТВ

В статье рассмотрены проблемы распространения IoT-устройств. Выявлены проблемы, которые мешают широкому распространению и применению IoT-устройств. Выполнен обзор системы Orvibo Zigbee Minihub EU и сделан вывод, что система не позволяет осуществлять сбор данных с любых IoT-устройств. Orvibo Zigbee Minihub EU позволяет использование только устройств с помощью собственного протокола Zigbee. Разработана программная реализация сбора информации от IoT-устройств с дальнейшей возможностью анализировать и обрабатывать полученные данные и выполнять запросы от данных устройств.

Ключевые слова: интернет, интернет вещей, IoT платформа, сеть устройств, умный дом, компьютерная система, безопасность, программное обеспечение.

O.V. Ivanchuk V.M. Kozel, Ie. A. Drozdova
Kherson National Technical University
E-mail: k_vic@ukr.net

RESEARCH OF IoT DEVICE COLLECTION SYSTEMS

The article discusses the problems of distribution of IoT devices. Identified problems that impede the widespread use of IoT devices. A review of the Orvibo Zigbee Minihub EU system was performed and it was revealed that the system does not allow data collection from any IoT devices. Orvibo Zigbee Minihub EU allows the use of only devices using its own Zigbee protocol. A software implementation was developed for collecting information from IoT devices with the further ability to analyze and process the received data and fulfill requests from these devices.

Keywords: internet, internet of things, IoT platform, device network, smart home, computer system, security, software.

Постановка проблемы. Каждый день разрабатываются новые устройства, которые имеют подключение к глобальной сети Интернет. В 2009 году количество устройств, которые имеют подключение к сети Интернет, сравнялось с количеством населения Земли, из-за чего «интернет людей» стал «интернетом вещей». Уже в 2017 году количество таких устройств достигло 20 млрд. По прогнозам компании Cisco вскоре количество устройств, которые имеют подключение к сети Интернет, будет составлять 50 млрд.

Большое количество разработчиков включают в свои устройства элементы «умного дома» для выполнения действий, указанных пользователем, с использованием подключения к сети Интернет.

Со временем количество устройств с элементами «умного дома» увеличивается, и это привело к тому, что создаются системы взаимодействия между устройствами для реагирования одних устройств на события из других устройств.

Системы, в которых происходит обмен данными между приборами, получили название «Интернет вещей» (Internet of Things, IoT). В таких системах вся аппаратура может обмениваться данными через сеть Интернет напрямую или через концентратор, который имеет подключение к сети Интернет.

Используя мобильные приложения или Web-страницы, пользователь может получить доступ к концентратору и выполнить настройку IoT-устройства или выбрать команду для выполнения. При этом нет необходимости в присутствии возле концентратора, достаточно иметь доступ к сети Интернет и знать IP адрес или Web адрес для подключения к концентратору.

Анализ последних исследований и публикаций. Интернет вещей - это всемирная паутина, в которой электронные устройства общаются между собой без вмешательства человека. IoT-устройства могут выполнять сбор информации о внешней среде, выполнять передачу собранных данных и производить их обработку [1]. Использование этих возможностей позволяет выполнить автоматизацию некоторых действий из повседневной жизни человека.

На данное время существует несколько проблем, которые мешают широкому распространению IoT-устройств, это [2]:

- проблемы выполнения удаленного подключения;
- проблема безопасности [3];
- проблема стандартизации.

Для выполнения подключения к сети Интернет устройство должно получить собственный IP-адрес. На сегодняшний день наиболее распространенным является стандарт IPv4, который может выдать примерно 4,22 миллиарда адресов, но количество устройств, которые могут выполнить подключение к сети Интернет, уже больше числа имеющихся адресов.

Проблема безопасности Интернета вещей состоит в возможности проникновения в системы умного дома или в сети предприятия через IoT-устройство. Предыдущие разработки компьютерных систем создавались с учетом изолированной среды. Однако IoT-устройства нуждаются в постоянном доступе к сети для взаимодействия друг с другом.

Формулирование цели исследования. Целью работы является исследование использования IoT-устройств, выявление проблем, которые мешают широкому распространению IoT-устройств, а также разработка системы, которая будет выполнять сбор и передачу данных с IoT-устройств с использованием одного IP-адреса.

Изложение основного материала исследования. Для IoT-устройств безопасность состоит, прежде всего, в целостности кода, проверке аутентичности пользователей, установления прав владения, а также возможности отражения виртуальных и физических атак. Однако большинство работающих сегодня IoT-устройств не обеспечены элементами защиты, имеют доступные извне интерфейсы управления, стандартные пароли, то есть, имеют все признаки Web-уязвимости [2,4].

Поскольку Интернет вещей - молодой и потенциально очень емкий рынок, такие компании, как Google, Intel, Apple, Microsoft предлагают свои платформы для него.

Каждая разработка новой платформы создает новый стандарт, из-за чего разработчикам IoT-устройств приходится решать проблему выбора стандарта, на основании которого устройство будет работать. Это создает проблему отсутствия совместимости со всеми остальными платформами.

Обмен данными с IoT-устройствами может производится с использованием следующих технологий:

- Bluetooth [5];
- Wi-Fi [6,7,8];
- Радиоканал на 315 или 433 Мгц [6].

Таким образом, для решения поставленных проблем необходимо разработать систему, которая будет выполнять сбор и передачу данных с IoT-устройств с использованием одного IP-адреса и иметь защиту от атак через сеть.

На рисунке 1 показано взаимодействие IoT-устройств с системой сбора данных.

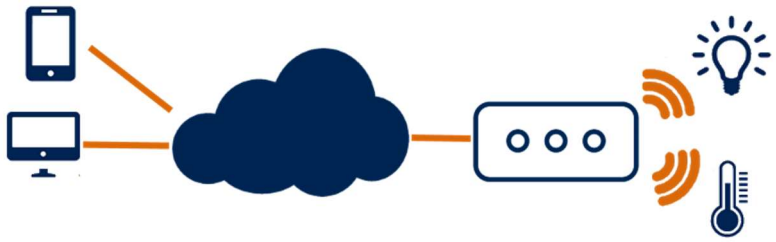

Рис. **Ошибка! Текст указанного стиля в документе отсутствует.** Связь IoT-устройств с системой сбора данных.

Система выполняет сбор данных от IoT-устройств через радиоканал на частоте 433 Мгц. Использование такого метода передачи данных обеспечит совместимость с большим количеством устройств [4]. Такой метод связи облегчает наладку и сбор данных. Использование такой системы позволит избежать проблемы адресации каждого IoT-устройства, поскольку будет необходим лишь один адрес для получения данных от всех IoT-устройств.

Предлагаемая система передачи имеет защиту в виде шифрования данных, которая обеспечит отсутствие внешнего влияния на данные и защиту IoT-устройств от внешнего вмешательства.

Примером реализации данной системы является система Orvibo Zigbee Minihub EU. Для обмена данными с IoT-устройствами используются ретрансляторы, которые могут создавать дополнительные препятствия при обмене данными из-за наличия дополнительных передатчиков. На рисунке 2 изображена связь с IoT-устройствами при использовании ретрансляторов.

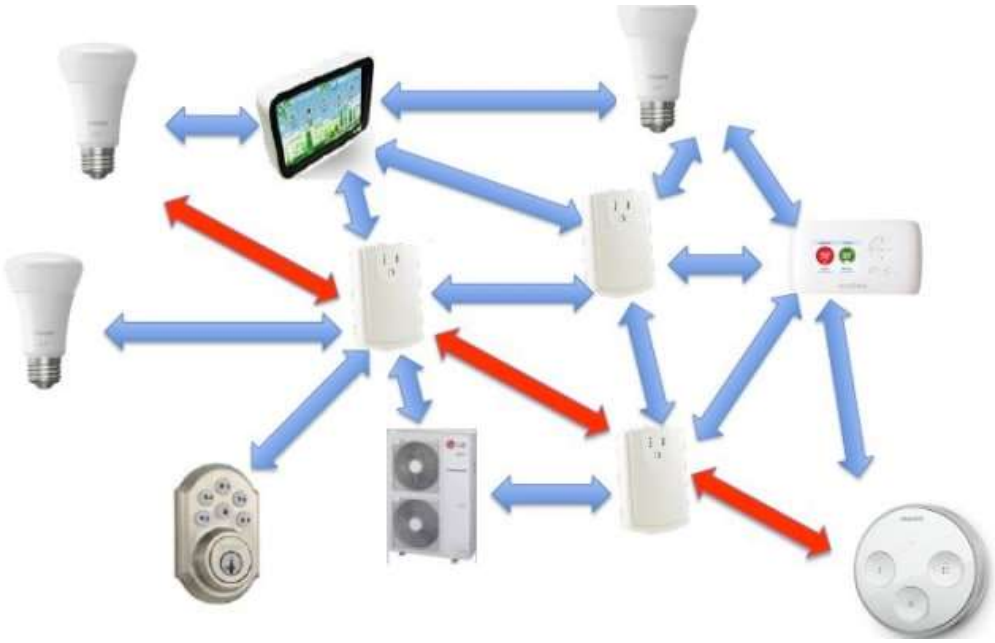

Рис. 2 Использование ретрансляторов в протоколе Zigbee

Для взаимодействия с системой используется сеть Wi-Fi. Также система имеет поддержку протокола Zigbee. Zigbee является протоколом верхнего уровня, который базируется на беспроводном стандарте IEEE 802.15.4. Наличие протокола ограничивает диапазон вновь подключаемых IoT-устройств, поскольку необходимо будет использовать только приборы с поддержкой данного протокола. Сама система нуждается в использовании аппаратуры с одинаковой версией протокола, из-за чего уменьшается количество устройств, которые можно использовать.

Система Orvibo Zigbee Minihub EU не позволяет выполнять сбор данных с любых IoT-устройств из-за необходимости использования только протокола Zigbee. Таким образом, разработка системы, которая будет выполнять сбор данных и не будет ограничена только устройствами, работающими по одному протоколу, является актуальной и необходимой. Для решения данной задачи было спроектировано устройство на базе микропроцессора и разработано программное обеспечение.

В начале работы программы необходимо выбрать IP-адрес подключения, через которое будет происходить обмен данными с устройством. После выбора адреса необходимо нажать кнопку «Подключение». После успешного подключения будет выполнена загрузка данных из устройства.

В левой части окна располагается меню страниц. При помощи нажатия на кнопки меню выполняется переход на соответствующую страницу. На рисунке 3 представлена страница событий в программе Liothubapp.

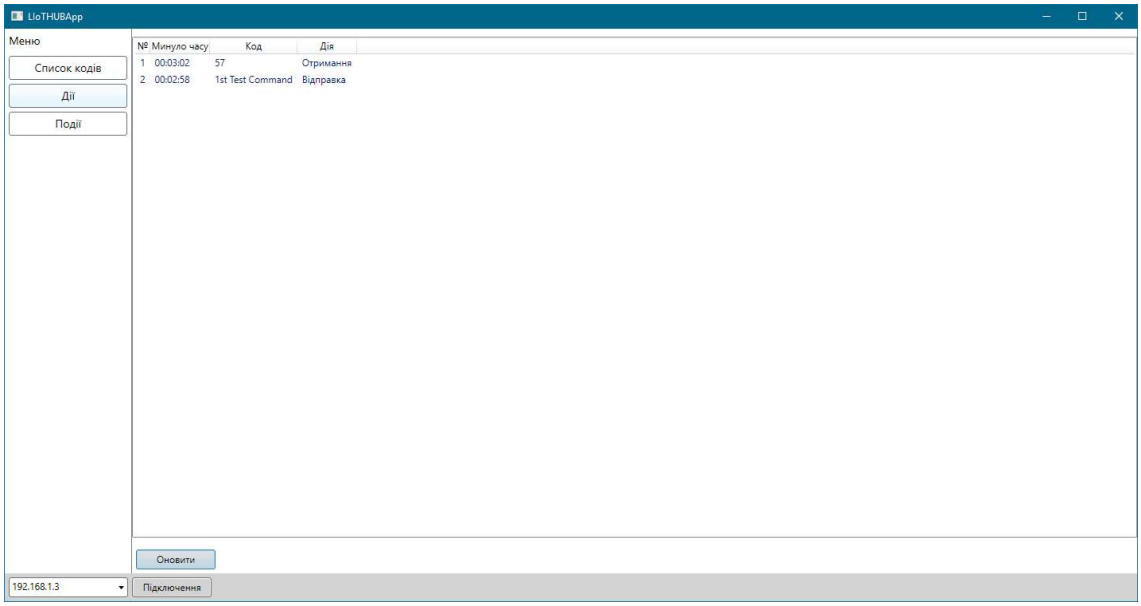

Рис. 3 Страница событий

На странице кодов можно для каждого кода задать уникальное имя для облегчения взаимодействия с кодами. Также можно выполнить запрос на поиск IoT-устройств. Если IoT-устройство в это время выполняет передачу кода, то система зафиксирует его в своей памяти и сможет с ним взаимодействовать.

На странице действий можно добавить соответствующую команду при получении определенного кода, которая позволит автоматизировать взаимодействие с другими IoT-устройствами. На странице событий можно просмотреть последние события, которые происходили с IoT-устройствами.

Выводы. Разработанный программно-аппаратный комплекс позволяет использовать протокол передачи данных через Wifi канал от разных IoT устройств. Дальнейшее усовершенствование программного обеспечения для разработанной системы позволит повысить безопасность сетей с помощью современных алгоритмов шифрования.

ПЕРЕЧЕНЬ ССЫЛОК

1. Грінгард С. Інтернет речей / Грінгард С.; пер. Герасимчук О. — м. Харків : Книжковий Клуб «Клуб Сімейного Дозвілля», 2018. – 176 с. ISBN 978-617-12-4657-7
2. Павел Притула. 5 проблем интернета вещей, которые предстоит решить. / Павел Притула [Електронний ресурс] Режим доступа URL: http://cnews.ru/link/a4631.
3. Бирюков А.А. Информационная безопасность: Защита и нападение. – 2-е изд., перераб. и доп. / Бирюков А.А. – М.: ДМК Пресс, 2017. - 434 с. ISBN 978-5-97060-435-9
4. David Rose. Enchanted Objects: Design, Human Desire, and the Internet of Things / David Rose. – New York : Scribner, 2014. – 320 p.
5. Simon Monk. Programming Arduino: Getting Started with Sketches : Second Edition / Simon Monk. – New York : McGraw-Hill, 2016. – 192 p.
6. Jeremy Blum. Exploring Arduino: Tools and Techniques for Engineering Wizardry / Jeremy Blum. – New York : Wiley, 2013. – 384 p.
7. John Boxall. Arduino Workshop: A Hands-On Introduction with 65 Projects / John Boxall. – San Francisco : No Starch Press, 2013. – 392 p.

8. James Kurose. Computer Networking: A Top-Down Approach : 7th Edition / James Kurose, Keith Ross. – London : Pearson, 2016. – 864 p.
9. Andrew Blum. Tubes: A Journey to the Center of the Internet / Andrew Blum. – New York : Ecco, 2013. – 304 p.
10. Marc Goodman. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World / Marc Goodman. – New York : Anchor, 2016. – 608 p.
11. Foster Provost. Data Science for Business: What You Need to Know about Data Mining and Data-Analytic Thinking / Foster Provost, Tom Fawcett. – Sebastopol : O`Relly Media, 2013. – 414 p.
12. Michael Howard. 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them / Michael Howard, David LeBlanc, John Viega. – New York : McGraw-Hill Osborne Media, 2010. – 443 p. ISBN: 978-0-07-162676-7