УДК 004.031.4 https://doi.org/ 10.35546/kntu2078-4481.2019.3.14

В.М. КОЗЕЛ
Херсонський національний технічний університет
ORCID: 0000-0002-2627-2499
О.В. ІВАНЧУК
Херсонський національний технічний університет
ORCID: 0000-0002-2058-4707
Є.А. ДРОЗДОВА
Херсонський національний технічний університет
ORCID: 0000-0003-0276-6387

РОЗРОБКА СИСТЕМИ ЗБОРУ ІНФОРМАЦІЇ ВІД IoT ПРИСТРОЇВ

У статті розглянуто проблеми поширення IoT-пристроїв. Виконано дослідження використання IoT-пристроїв. Виявлені проблеми, що заважають широкому застосуванню IoT-пристроїв. Виконано огляд системи Orvibo Zigbee Minihub EU та виявлено, що система не дозволяє виконувати збір даних з будь-яких IoT-пристроїв. Orvibo Zigbee Minihub EU дозволяє їхнє використання лише за допомогою власного протоколу ZigBee. Через це прийняте рішення розробити систему, що виконуватиме збір даних та не буде мати обмежень щодо роботи за одним протоколом. Розроблено програмно-апаратну систему, що виконуватиме збір та передачу даних з IoT-пристроїв, яка матиме одну IP-адресу, а також програмну реалізацію збору інформації з IoT-пристроїв з подальшою можливістю аналізувати та обробляти отримані дані і виконувати запити від даних пристроїв. Для запропонованої системи розроблено структурну схему на базі мікроконтролера ATMega328p для обміну даними між IoT-пристроями. Для роботи системи розроблено програмне забезпечення для пристрою та комп'ютеру, яке дозволяє на сторінці кодів задавати для кожного коду унікальне ім'я, для полегшення взаємодії з кодами. Також програмне забезпечення виконує запит на пошук IoT-пристроїв. Якщо IoT- пристрій у цей час виконує передачу коду, то пристрій зафіксує його у своєї пам'яті та зможе з ним взаємодіяти. На сторінці дій можна додати відповідну дію при отриманні певного коду, що дозволить автоматизувати дії, пов'язанні з IoT-пристроями. Програма дозволяє переглянути останні події, що відбулися з IoT-пристроями.

Розроблена система збору інформації дозволяє використовувати протокол передачі даних від різних IoT пристроїв через Wi-Fi канал. Зважаючи на те, що застосований в спроектованій системі мікроконтролер є цілком доступним, вартість даного пристрою значно менша ніж у рішень, які представлені нині на ринку пристроїв. Подальше удосконалення програмного забезпечення для розробленої системи дозволить підвищити безпеку мереж за допомогою сучасних алгоритмів шифрування.

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

В.Н. КОЗЕЛ
Херсонский национальный технический университет
ORCID: 0000-0002-2627-2499
А.В. ИВАНЧУК
Херсонский национальный технический университет
ORCID: 0000-0002-2058-4707
Е.А. ДРОЗДОВА
Херсонский национальный технический университет
ORCID: 0000-0003-0276-6387

РАЗРАБОТКА СИСТЕМЫ СБОРА ИНФОРМАЦИИ ОТ IoT УСТРОЙСТВ

В статье рассмотрены проблемы распространения IoT-устройств. Выполнены исследования использования IoT-устройств. Выявлены проблемы, мешающие широкому применению IoT-устройств. Выполнен обзор системы Orvibo Zigbee Minihub EU и выявлено, что система не позволяет выполнять сбор данных с любых IoT-устройств. Orvibo Zigbee Minihub EU позволяет их использование только с помощью собственного протокола ZigBee. Поэтому принято решение разработать систему, которая будет выполнять сбор данных, но не будет иметь ограничений для работы по одному протоколу. Разработана программно-аппаратная система, которая будет выполнять сбор и передачу данных с IoT-устройств и будет иметь один IP-адрес, а также программная реализация сбора информации с IoT-устройств с последующей возможностью анализировать и обрабатывать полученные данные и выполнять запросы от данных устройств. Для предложенной системы разработана структурная

схема на базе микроконтроллера ATMega328p для обмена данными между IoT устройствами. Для работы системы разработано программное обеспечение для устройства и компьютера, которое позволяет на странице кодов задавать для каждого кода уникальное имя, для облегчения взаимодействия с кодами. Также программное обеспечение выполняет запрос на поиск IoT-устройств. Если IoT- устройство в это время выполняет передачу кода, то устройство зафиксирует его в своей памяти и сможет с ним взаимодействовать. На странице действий можно добавить соответствующее действие при получении определенного кода, что позволит автоматизировать действия, связанные с IoT устройствами. Программа позволяет просмотреть последние события, произошедшие с IoT устройствами.

Разработаная система сбора информации позволяет использовать протокол передачи данных от различных IoT устройств используя Wi-Fi канал. Благодаря тому, что примененный в спроектированной системе микроконтроллер является доступным, стоимость данного устройства значительно меньше, чем у решений, которые представлены сейчас на рынке устройств. Дальнейшее совершенствование программного обеспечения для разработанной системы позволит повысить безопасность сетей с помощью современных алгоритмов шифрования.

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

V.M. KOZEL
Kherson National Technical University
ORCID: 0000-0002-2627-2499
O.V. IVANCHUK
Kherson National Technical University
ORCID: 0000-0002-2058-4707
Ye.A. DROZDOVA
Kherson National Technical University
ORCID: 0000-0003-0276-6387

DEVELOPMENT OF SYSTEM FOR COLLECTING INFORMATION FROM IoT DEVICES

The article discusses the problems of distribution of IoT devices. A study on the use 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 determined that the system does not allow data collection from arbitrary IoT devices. Orvibo Zigbee Minihub EU allows the use of IoT devices only using its own ZigBee protocol. In connection with this, a system was developed that performs data collection and does not require devices designed to operate on a single protocol. A hardware and software system has been developed that collects data from IoT devices and has one IP address, as well as a software implementation of data collection from IoT devices with the further ability to analyze and process the received data, and perform requests from these devices. For the proposed system, a block diagram has been developed based on the ATMega328p microcontroller for exchanging data between IoT devices. For the system to work, software was developed for the device and the computer, which allows you to set a unique name for each code, which simplifies interaction with codes. The software also performs a search request for IoT devices. When the IoT device transfers the code, the system will fix it in its memory and will be able to interact with it. The hardware-software complex allows you to add the appropriate action when you receive a specific code, which allows you to automate actions associated with IoT devices. The program allows you to view the latest events that have occurred with IoT devices. The program allows you to view the latest developments with IoT-devices.

The developed information collection system allows the use of data transfer protocol from various IoT devices using Wi-Fi channel. Due to the fact that the microcontroller used in the designed system is affordable, the cost of this device is significantly less than the solutions that are currently on the device market. Further improvement of the software for the developed system will improve network security using modern encryption algorithms.

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

Постановка проблеми

Кожного дня розробляються нові пристрої, що мають підключення до глобальної мережі Інтернет. У 2009 році кількість пристроїв, підключених до Інтернет, зрівнялася з кількістю населення Землі, через що «інтернет людей» став «інтернетом речей». Вже у 2017 році кількість пристроїв досягла 20 млрд. По прогнозам компанії Cisco кількість пристроїв, що мають підключення до мережі Інтернет, в найближчий час складе 50 млрд.

Велика кількість розробників включає до своїх пристроїв елементи «розумного будинку» для виконання дій, вказаних користувачем, через підключення до мережі Інтернет.

Зважаючи на постійне зростання кількості пристроїв з елементами «розумного будинку», корпорації почали розробку систем взаємодії між ними для реагування одних пристроїв на події з інших пристроїв.

Системи, в яких відбувається обмін даними між пристроями, отримали назву «Інтернет речей». В таких системах усі пристрої здатні на обмін даними з мережею Інтернет напряму або через концентратор, що має підключення до глобальної мережі.

Використовуючи мобільні додатки або WEB-сторінки, користувач може отримати доступ до концентратора та виконати налаштування IoT-пристроїв, або обрати команду для виконання ними. При цьому немає необхідності присутності біля концентратора, достатньо мати доступ до мережі Інтернет та знати IP чи WEB адресу для підключення до концентратора.

Аналіз останніх досліджень і публікацій

Інтернет речей (IoT) - це всесвітня павутина, в якій електронні пристрої спілкуються між собою без втручання людини. IoT-пристрої можуть виконувати збирання інформації про зовнішнє середовище, передачу зібраних даних та їхню обробку [1]. Використання цих можливостей дозволяє автоматизувати деякі дії з повсякденного життя людини.

На даний час є кілька проблем, що заважають подальшому поширенню IoT-пристроїв [2]:

- проблеми виконання віддаленого підключення;
- проблема безпеки [3];
- проблема стандартизації.

Для підключення до мережі Інтернет пристрій має отримати власну IP-адресу. Наразі найпоширенішим є стандарт IPv4, який може видати близько 4,22 мільярда адрес. Але кількість пристроїв, що потенційно можуть здійснювати підключення до мережі Інтернет, вже більше кількості наявних адрес.

Наявність проблеми безпеки Інтернету речей призводить до можливості несанкціонованого проникнення до систем будинків або до мережі підприємства через IoT-пристрої.

Якщо раніше розробка комп'ютерних систем традиційно велася з урахуванням ізольованого середовища, то нині IoT-пристрої потребують постійного доступу до глобальної мережі для взаємодії з іншими пристроями.

Формулювання мети дослідження

Метою роботи було дослідження використання IoT-пристроїв для виявлення проблем, що заважають їхньому подальшому поширенню, та розробка системи, що виконуватиме збір та передачу даних з IoT-пристроїв, і при цьому матиме одну IP-адресу.

Викладення основного матеріалу дослідження

Для IoT-пристроїв безпека гарантується, перш за все, цілісністю коду, перевіркою автентичності користувачів (пристроїв), встановленням права володіння, а також можливістю відбиття віртуальних і фізичних атак. Але більшість IoT-пристроїв, що працюють сьогодні, не забезпечені елементами захисту, мають доступні ззовні інтерфейси управління, стандартні паролі, тобто, мають всі ознаки веб-уразливості [2,4].

Оскільки Інтернет речей – молодий і потенційно дуже ємний ринок, такі компанії-лідери ринку, як Google, Intel, Apple, Microsoft пропонують свої платформи для цієї технології.

Кожна розробка нової платформи створює новий стандарт, через що розробникам IoT-пристроїв доводиться обирати з наявної безлічі єдиний стандарт, за яким пристрій буде працювати. Це створює проблему відсутності сумісності між усіма платформами.

Обмін даними з IoT-пристроями може виконуватися за технологіями:

- Bluetooth [5];
- Wi-Fi [6,7,8];
- Радіоканал на частоті 315 або 433 МГц [6].

Вирішенню цих проблем сприятиме розробка системи, що буде виконувати збір та передачу даних (рис.1) з IoT-пристроїв. Особливістю розроблюваної системи є те, що вона має використовувати одну IP-адресу та буде захищеною від атак через мережу.

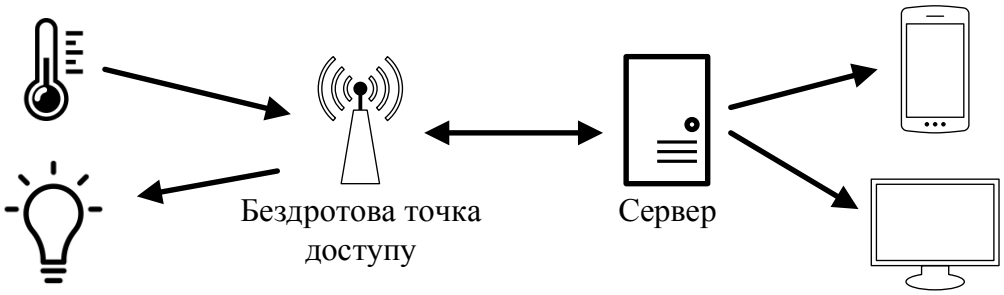

Рис. 1. Зв'язок IoT-пристроїв з системою збору даних

Пристрій виконує збір даних з IoT-пристроїв через радіоканал на частоті 433 МГц. Використання такого методу передачі даних забезпечить сумісність з великою кількістю пристроїв [4] і полегшить налаштування та збір даних. Впровадження системи дозволить уникнути проблеми адресації кожного IoT-пристрою, оскільки для отримання даних з усіх IoT-пристроїв буде необхідна лише одна адреса.

Пропонована система передачі має захист у вигляді шифрування даних, що забезпечить відсутність зовнішнього впливу на дані та гарантує захист IoT-пристроїв від зовнішнього втручання.

Прикладом реалізації подібного підходу є система Orvibo Zigbee Minihub EU. Для обміну даними з IoT-пристроями використовуються ретранслятори (рис. 2), що можуть створювати додаткові перешкоди при обміні даними через наявність додаткових передавачів.

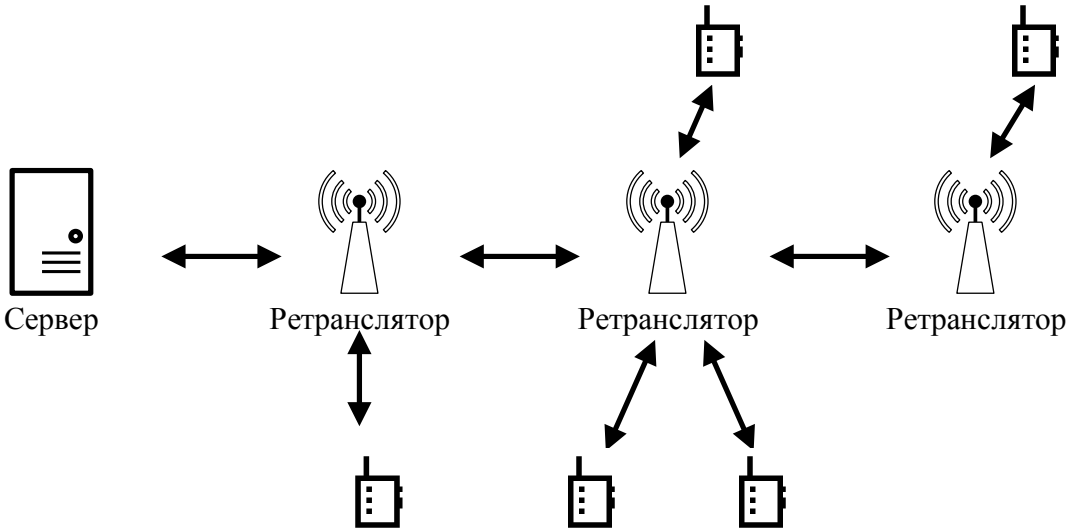

Рис. 2. Використання ретрансляторів в протоколі ZigBee

Для взаємодії з системою використовується мережа Wi-Fi. Також система має підтримку протоколу ZigBee. ZigBee є протоколом верхнього рівня, що базується на бездротовому стандарті IEEE 802.15.4. Наявність протоколу створює проблему вибору IoT-пристроїв, оскільки необхідно використовувати IoT-пристрої лише з підтримкою цього протоколу. Сама система потребує використання пристроїв з однаковою версією протоколу, через що зменшується кількість пристроїв, які можуть бути підключені до системи.

Через те, що система Orvibo Zigbee Minihub EU значно обмежує коло потенційно придатних для підключення до неї IoT-пристроїв через необхідність використання лише протоколу ZigBee, було прийняте рішення розробити систему, що виконуватиме збір даних з пристроїв, створених для роботи за різними протоколами.

На основі аналізу принципів роботи та обміну даними між IoT-пристроями була розроблена структурна схема пристрою (рис. 3), на якій зображені основні блоки та їхня взаємодія.

Пристрій має такі основні блоки:

- Мікроконтролер ATMega328p;
- Мікроконтролер ESP8266;
- Передавач MX-05V;

– Приймач MX-RF-5V (XD-RF-5V);

Допоміжні блоки пристрою:

– Стабілізатор напруги LM7805;
– Стабілізатор напруги LM1117-3.3v;
– Кварцовий резонатор 16 МГц;

Опис роботи пристрою.

Робота пристрою починається з подачі живлення на стабілізатор напруги DA1. Він виконує зниження напруги до 5В. Напруга у 5В подається на елементи DA2, DD1 та модулі XD-RF-5V, MX-05V.

Стабілізатор напруги DA2 виконує зменшення напруги до 3,3В. Напруга у 3,3В подається на модуль ESP8266 [6].

Після подачі напруги, модулі ESP8266, MX-05V, XD-RF-5V очікують команди ініціалізації від мікроконтролера DD1.

Мікроконтролер DD1 виконує запуск програмного коду з внутрішньої пам'яті.

При старті програми виконується передача команд на модуль ESP8266 для ініціалізації Wi-Fi мережі. Після підтвердження ініціалізації Wi-Fi мережі від модуля ESP8266, мікроконтролер DD1 виконує ініціалізацію модулів XD-RF-5V, MX-05V.

Отримавши підтвердження ініціалізації модулів, мікроконтролер DD1 очікує передачу даних з Wi-Fi мережі чи з модулю MX-RF-5V.

Коли від Wi-Fi мережі чи від IoT-пристроїв через радіоканал дані надходять до мікроконтролера DD1, він виконує їхню обробку. При отримані даних з Wi-Fi мережі відбувається обробка запиту. Після обробки запиту мікроконтролер DD1 відправляє відповідь, якщо вона є необхідною згідно запиту [7,11].

Для роботи з системою розроблене програмне забезпечення (рис. 4), до складу якого входить програма для системи збору інформації від IoT пристроїв та програма віддаленого керування системою.

На початку роботи програми віддаленого керування необхідно обрати IP-адресу підключення, через яке відбуватиметься обмін даними з пристроєм. Після вибору адреси необхідно натиснути кнопку «Підключення». Після успішного підключення буде виконане завантаження даних з пристрою.

В лівій частині вікна знаходиться меню сторінок. Шляхом натискання на кнопки меню відбувається перехід на відповідну сторінку.

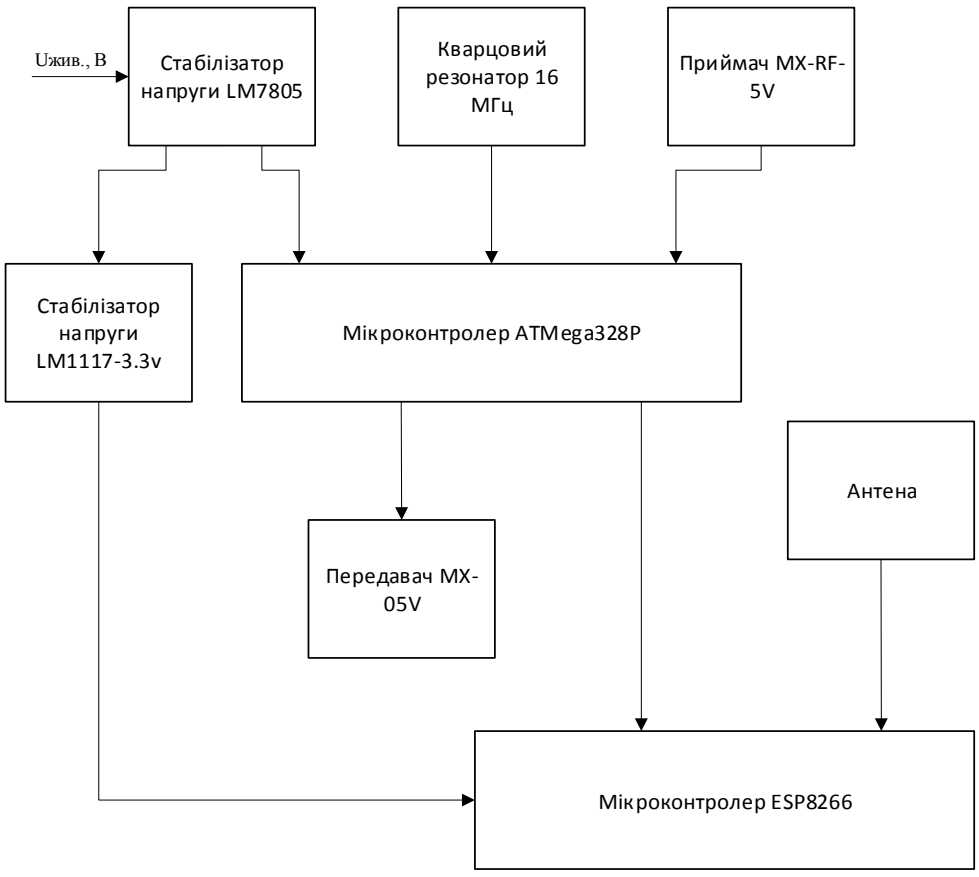

Рис. 3. Структурна схема пристрою

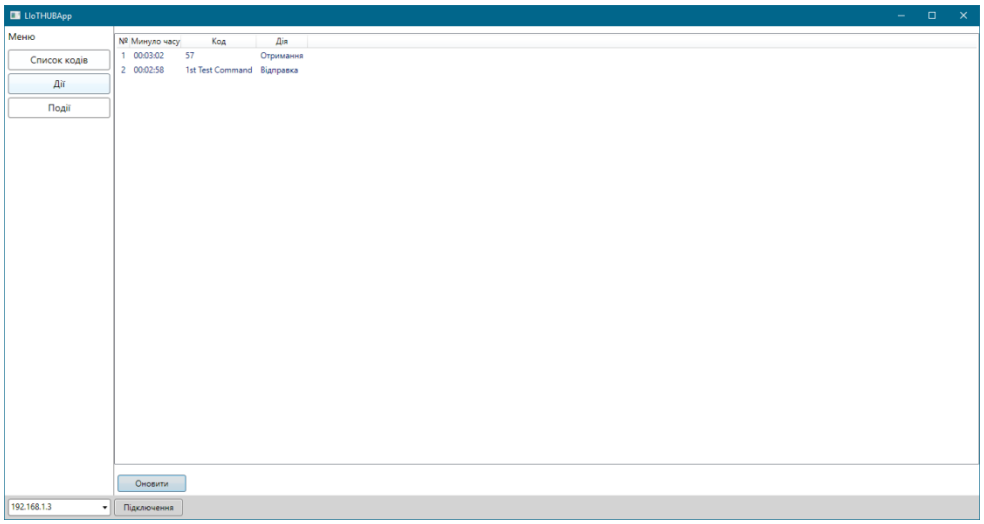

Рис. 4. Сторінка подій

На сторінці кодів можна задати для кожного коду унікальне ім'я, для полегшення взаємодії з кодами. Також можна виконати запит на пошук IoT-пристроїв. Якщо IoT- пристрій у цей час виконує передачу коду, то пристрій зафіксує його у своєї пам'яті та зможе з ним взаємодіяти.

На сторінці дій можна додати відповідну дію при отриманні певного коду, що дозволить автоматизувати дії, пов'язані з IoT-пристроями. На сторінці подій можна переглянути останні події, що відбулися з IoT-пристроями.

Висновки

Розроблена система збору інформації дозволяє використовувати протокол передачі даних від різних IoT пристроїв через Wi-Fi канал. Зважаючи на те, що застосований в спроектованій системі мікроконтролер є цілком доступним, вартість даного пристрою значно менша ніж у рішень, які представлені нині на ринку пристроїв. Подальше удосконалення програмного забезпечення для розробленої системи дозволить підвищити безпеку мереж за допомогою сучасних алгоритмів шифрування.

Список використаної літератури

1. Семюел Грінгард Інтернет речей / пер. з англ. О.А. Герасимчук. Харків : Книжний Клуб «Клуб Сімейного Дозвілля», 2018. – 176 с.
2. 5 проблем интернета вещей, которые предстоит решить. [Электронный ресурс]/Режим доступа: http://cnews.ru/link/a4631 (дата звернення 07.05.2019).
3. Андрей Бирюков. Информационная безопасность: Защита и нападение. М.: ДМК-Пресс, 2017. – 434 с.
4. David Rose. Enchanted Objects: Design, Human Desire, and the Internet of Things. New York : Scribner, 2014. – 320 p.
5. Tom Igoe. Making Things Talk: Using Sensors, Networks, and Arduino to See, Hear, and Feel Your World. Sebastolpol : Maker Media, 2017. – 496 p.
6. Marco Schwartz. Internet of Things with ESP8266. Birmingham : Packt Publishing, 2016. – 226 p.
7. Howard Johnson. High-Speed Signal Propagation: Advanced Black Magic. New Jersey : Prentice Hall, 2003. – 808 p.
8. Mark Geddes. Arduino Project Handbook: 25 Practical Projects to Get You Started. San Francisco : No Starch Press, 2016. – 272 p.
9. Brian Huang. Derek Runberg. The Arduino Inventor's Guide: Learn Electronics by Making 10 Awesome Projects. San Francisco : No Starch Press, 2017. – 335 p.
10. Howard Johnson. High-Speed Digital Design: A Handbook of Black Magic. New Jersey : Prentice Hall, 1993. 464 p.
11. Simon Monk. Programming Arduino: Getting Started with Sketches : Second Edition. New York : McGraw-Hill, 2016. – 192 p.
12. Jeremy Blum. Exploring Arduino: Tools and Techniques for Engineering Wizardry. New York : Wiley, 2013. – 384 p.
13. John Boxall. Arduino Workshop: A Hands-On Introduction with 65 Projects. San Francisco : No Starch Press, 2013. – 392 p.

14. James Kurose, Keith Ross. Computer Networking: A Top-Down Approach : 7th Edition. London : Pearson, 2016. – 864 p.
15. Andrew Blum. Tubes: A Journey to the Center of the Internet. New York : Ecco, 2013. – 304 p.
16. Marc Goodman. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. New York : Anchor, 2016. – 608 p.
17. Foster Provost, Tom Fawcett. Data Science for Business: What You Need to Know about Data Mining and Data-Analytic Thinking. Sebastopol : O`Relly Media, 2013. – 414 p.
18. Michael Howard, David LeBlanc, John Viega. 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. New York : McGraw-Hill Osborne Media, 2005. – 304 p.

References

1. Greengard S. The Internet of Things. Cambridge, 2015. 230 p. (Ukr. ed.: Herasymchuk O.A. Internet rechei. Kharkiv, Knyzhnyi Klub «Klub Simeinoho Dozvillia», 2018. – 176 p.)
2. 5 problem interneta veschey, kotoryie predstoit reshit. (5 problems of the Internet of things to be solved) Available at: http://cnews.ru/link/a4631 (accessed 7 May 2019).
3. Biryukov A. Informatsionnaya bezopasnost: Zaschita i napadenie. Moscov [Information Security: Defense and Attack], DMK-Press, 2017. – 434 p.
4. Rose D. Enchanted Objects: Design, Human Desire, and the Internet of Things. New York, Scribner, 2014. 320 p.
5. Igoe T. Making Things Talk: Using Sensors, Networks, and Arduino to See, Hear, and Feel Your World. Sebastolpol, Maker Media, 2017. 496 p.
6. Schwartz M. Internet of Things with ESP8266. Birmingham, Packt Publishing, 2016. 226 p.
7. Johnson H. High-Speed Signal Propagation: Advanced Black Magic. New Jersey, Prentice Hall, 2003. 808 p.
8. Geddes M. Arduino Project Handbook: 25 Practical Projects to Get You Started. San Francisco, No Starch Press, 2016. – 272 p.
9. Huang B. Runberg D. The Arduino Inventor's Guide: Learn Electronics by Making 10 Awesome Projects. San Francisco, No Starch Press, 2017. – 335 p.
10. Johnson H. High-Speed Digital Design: A Handbook of Black Magic. New Jersey, Prentice Hall, 1993. – 464 p.
11. Monk S. Programming Arduino: Getting Started with Sketches, 2nd ed. New York, McGraw-Hill, 2016. – 192 p.
12. Blum J. Exploring Arduino: Tools and Techniques for Engineering Wizardry. New York, Wiley, 2013. – 384 p.
13. Boxall J. Arduino Workshop: A Hands-On Introduction with 65 Projects. San Francisco, No Starch Press, 2013. – 392 p.
14. Kurose J, Ross K. Computer Networking: A Top-Down Approach, 7th ed. London, Pearson, 2016. – 864 p.
15. Blum A. Tubes: A Journey to the Center of the Internet. New York, Ecco, 2013. – 304 p.
16. Goodman M. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. New York, Anchor, 2016. – 608 p.
17. Provost F, Fawcett T. Data Science for Business: What You Need to Know about Data Mining and Data-Analytic Thinking. Sebastopol, O`Relly Media, 2013. – 414 p.
18. Howard M, LeBlanc D, Viega J. 19 Deadly Sins of Software Security: Programming Flaws and How to Fix Them. New York, McGraw-Hill Osborne Media, 2005. – 304 p.