УДК 004.738.5:004.722]:004.052

НАДІЙНІСТЬ ІОТ-МЕРЕЖ

Русінов Ю. М.
Науковий керівник — к.т.н., проф. Немченко В. П.
Харківський національний університет радіоелектроніки, каф. АПОТ,
м. Харків, Україна
тел. +38(097) 177-88-70

The wide spread of the Internet of Things is facilitated by the mass appearance of devices equipped with electronic components, software and communication capabilities. The entire industry is on the path of making life easier for people, developing automated systems that work almost without human intervention. But of course there must be ways to control these devices. Any electronics can contain software or hardware errors that must be resolved in a short time. It is very important to analyze the security issues and identify the possible risks of IoT and to investigate the existing methods of ensuring information security.

Вступ. Інтернет речей (Internet of Things, IoT) — найшвидше зростаюча технологічна галузь. У промисловості технології Інтернету речей застосовуються для оптимізації оперативних витрат, збільшення терміну експлуатації продуктів та покращення добробуту людей. «Речами» в Інтернеті речей є глибоко вбудовані пристрої з такими відмітними особливостями, як вузька смуга пропускання, збір даних з низькою повторюваністю і малий обсяг використовуваних даних. Ці пристрої обмінюються даними один з одним і надають дані через інтерфейси.

Зміст дослідження. Архітектури IoT різняться за складністю та кількістю архітектурних шарів залежно від конкретного бізнес-завдання, проте комітет з архітектури Всесвітнього форуму IoT, складений з лідерів індустрії, включаючи IBM, Intel і Cisco, в жовтні 2014 опублікував еталонну модель IoT, що має 7 шарів: фізичні пристрої та контролери; зв'язок; туманні обчислення; накопичення даних; абстракція даних; додатки; взаємодія та процеси.

Технологіями, що використовуються в системах IoT, є: периферійні обчислення, хмарні обчислення та машинне навчання.

Периферійні обчислення (інша назва — «Туманні обчислення, fog computing») відносять до технології, яку використовують для того, щоб інтелектуальні пристрої могли робити більше, ніж просто надсилати або отримувати дані на свою платформу IoT. Тобто, цей шар є проміжним між IoT-платформою та «зовнішнім світом». Хмарними обчисленнями. Це збільшує обчислювальну потужність на периферії мережі IoT, зменшуючи затримку зв'язку та покращуючи час відповіді.

Хмарні технології використовуються для віддаленого зберігання даних та керування пристроями IoT, що робить дані доступними для кількох

пристроїв у мережі.

Машинне навчання відноситься до ПЗ та алгоритмів, що використовуються для обробки даних та прийняття рішень у режимі реального часу на основі цих даних. Алгоритми машинного навчання можна розгорнути у хмарі чи периферії.

Безпеку Інтернету речей можна побудувати на фундаменті із чотирьох наріжних каменів: безпека зв'язку, захист пристроїв, контроль пристроїв та контроль взаємодій у мережі. Канал зв'язку повинен бути захищений, для цього застосовуються технології шифрування та автентифікації, щоб збільшити довіру до віддаленої системи. Важливим завданням також є керування ключами для перевірки автентичності даних та достовірності каналів їх отримання. Провідні центри сертифікації вже вбудували «сертифікати пристроїв» у понад мільярд пристроїв IoT, надавши можливість виконувати перевірку справжності широкого спектру пристроїв. Захист пристроїв — забезпечення безпеки та цілісності програмного коду. Підписання коду підтверджує правомірність його запуску, також необхідний захист під час виконання коду, щоб атакуючі не перезаписували його під час завантаження.

Неможливо повністю позбавитися вразливості в пристроях IoT. Їх необхідно усувати, і це може відбуватися протягом тривалого часу після передачі обладнання споживачеві. Механізм оновлення через повітря (over-the-air) вимагає програмне та апаратне забезпечення, що підтримує таке оновлення, а саме потрібна підтримка отримання та встановлення патчів, отриманих через бездротову мережу від провайдера. Зазвичай нове ПЗ встановлюється, замінюючи застарілі файли на нові версії.

Деякі загрози зможуть подолати будь-які вжиті заходи незалежно від того, наскільки добрим є захист. Тому важливо мати можливості аналітики безпеки в IoT. Системи для аналітики безпеки допоможуть краще зрозуміти мережу, помітити підозрілі, небезпечні чи зловмисні аномалії.

Висновки. Підвищення безпеки інтернету речей є першорядною задачею при розробці сучасною IoT-технології. Вище розглянуто її важливі складові і вказано напрямки її розвитку.

Список використаних джерел:

1. AWS. What is IoT? https://aws.amazon.com/what-is/iot/

2. Бізнес майстерня. Інтернет речей: мережева архітектура та архітектура безпеки. https://www.bizmaster.xyz/2020/12/internet-rechei-merezheva-arkhitektura-ta-arkhitektura-bezpeky.html

3. Гіоргізова-Гай, В. Ш., Шеренковський, А. О. (2019). Шлюз у системі Інтернету речей. Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки, 30(69), 1, 31–37.

4. Nemchenko V., Schaff A. (2003) Vulnerabilities and test of Internet protocols. Radioelectronika i Informatika, 3, p.195–196.