УДК 004.056.5:004.056.57

АНАЛІЗ РОЛІ БЕЗПЕКИ В РОЗВИТКУ ІНТЕРНЕТУ РЕЧЕЙ

Ткаченко Є.М. – гр. БКІ-20, бакалавр, *eyva.tkachenko@gmail.com*
Стаценко В.В. – к.т.н., доц., *statsenko.v@knutd.edu.ua*
Київський національний університет технологій та дизайну

Мета роботи полягає в аналізі ролі безпеки в розвитку Інтернету речей (IoT) і визначенні ключових викликів, пов'язаних з цим аспектом технологічного прогресу. Також надається висновок щодо необхідності посилення заходів забезпечення безпеки та розробки відповідних стандартів для забезпечення стабільного та безпечного розвитку Інтернету речей.

Інтернет речей (IoT) - це глобальна взаємодія інтелектуальних пристроїв через Інтернет. IoT забезпечує можливість будь-яким пристроям з'єднуватися та обмінюватися даними, перетворюючи фізичний світ на величезну інформаційну систему. Різні технології, такі як хмарні обчислення та машинне навчання для аналізу даних і створення інформаційних моделей, швидко стають необхідною частиною інфраструктури IoT. Величезний прогрес у цій сфері також сприяє розвитку бізнесу в галузі інформаційно-комунікаційних технологій (ІКТ). Прогнозується, що до 2022 року 95% нових продуктів матимуть підтримку IoT, що свідчить про те, що IoT стане необхідною складовою нашого щоденного життя. [1]

У зв'язку з постійним зростанням числа IoT-пристроїв та їхньою доступністю до Інтернету, зростає обурення щодо безпеки, а саме, законного доступу користувачів до даних. Із одного боку, всепроникаючий характер IoT спонукає до створення інноваційних застосунків для кінцевих користувачів, але, з іншого боку, відсутність заходів забезпечення безпеки може призвести до критичних проблем, наприклад, крадіжки через вразливість у системах розумної сигналізації. Безпека також має інший аспект - "конфіденційність". Компанії, які управляють конфіденційними даними користувачів, можуть незаконно використовувати їх, що призводить до порушення конфіденційності.

Загострення ситуації пов'язане з тим, що лише кілька років тому існували малоймовірні сценарії розвитку IoT з мільярдами підключених пристроїв, тому аспекти безпеки не завжди враховувалися на етапі проектування продуктів. За даними досліджень, проведених Gartner, у 2018 році витрати на безпеку IoT по всьому світу склали 1,5 мільярда доларів США, і до 2022 року понад половину всіх бюджетів IoT буде спрямовано на усунення несправностей, відкликання пристроїв з ринку та вирішення проблем безпеки, а не на захист. [2]

На сьогоднішній день IoT використовується у таких галузях, як охорона здоров'я, промисловість, роздрібна торгівля, будівництво, розвиток міської інфраструктури, транспорт, енергетика та інші. За даними IHS Markit, передбачається, що до кінця 2030 року кількість підключених пристроїв IoT досягне 125 мільярдів. [3]

Поняття IoT інтегрується в наявну архітектуру мереж, використовуючи IP-мережі та хмарну інфраструктуру для забезпечення зв'язку між пристроями та додатками. Вони можуть обмінюватися інформацією як всередині приватних сегментів, так і між мережами, що оптимізує процеси для підвищення ефективності та забезпечення безпеки.

Для реалізації IoT найважливішими питаннями є безпека даних, довіра до мережі та ізоляція з'єднання.

1. Безпека даних: Великі втрати від вірусів, подібних тому, який був виявлений у 2010 році, демонструють необхідність надійної інфраструктури IoT. Безпека означає захист від пошкоджень, втрат, крадіжок та підробок даних.

2. Довіра до мережі: Після скандалу зі витоком даних у 2013 році в США важко довіряти партнерам та працівникам, що мають доступ до користувацьких даних. Довіра та анонімність є критичними для майбутнього IoT.

3. Контроль неізольованих з'єднань: Взаємодія пристроїв всередині локального сегмента IoT мережі потребує уваги, оскільки вони повинні взаємодіяти з усією екосистемою IoT. Контроль за неізольованими з'єднаннями є ключовою проблемою, що потребує вирішення.

Висновок. У світлі швидкого росту кількості пристроїв IoT та їхнього поширення в усі сфери життя, безпека стає не лише питанням технологічного розвитку, але й національної та глобальної безпеки. Недоліки в захисті даних та вразливості мереж можуть призвести до серйозних наслідків, що ставить під загрозу як індивідуальність, так і економічну стабільність. Тому постійне вдосконалення систем безпеки та розвиток відповідних стандартів стають невід'ємною частиною розвитку IoT. Тільки шляхом спільних зусиль технічних спеціалістів, виробників, урядових структур та споживачів можна забезпечити стабільний та безпечний розвиток Інтернету речей, який принесе користь усьому суспільству.

Література

1. Тихвінський В.О., Бочечка Г.С., Нургожин Б.І., Айтмагамбетов А.З. Мережі IoT/M2M: технології, програми та регулювання. 2016.

2. Newsroom G. Gartner Says Worldwide IoT Security Spending Will Reach $1 Billion in 2018 // Gartner. - 2017. URL: https://www.gartner.com/newsroom/id/

3. The Internet of Things: a movent, not a market // IHS Markit. - 2018. URL: http://cdn.ihs.com/www/pdf/IoT_ebook.pdf