5. Оцінка складності алгоритмів, або Що таке O(log n). URL: https://echo.lviv.ua/dev/53 (дата звернення: 21.12.2020).
6. Руденко В. Д., Речич Н. В., Потієнко В. О. Інформатика для загальноосвітніх навчальних закладів з поглибленим вивченням інформатики : підруч. для 9 кл. загальноосвіт. навч. закл. Харків : Вид-во «Ранок». 2017. 240 с.
7. Абрамов С. А., Гнездилова Г. Г., Капустина Е. Н., Селюн М. И. Задачи по программированию. Вологда, 2000. 596 с.
8. Perfect number. URL: https://en.wikipedia.org/wiki/Perfect_number (дата звернення: 21.12.2020).
9. Great Internet Mersenne Prime Search. URL: https://www.mersenne.org/ (дата звернення: 21.12.2020).
10. Теорія чисел – математичні основи розв'язування олімпіадних задач. URL: https://www.e-olymp.com/uk/blogs/posts/53 (дата звернення: 21.12.2020).
11. Креневич А. П., Обвінцев О. В. С у задачах і прикладах : навчальний посібник із дисципліни «Інформатика та програмування». Київ: Видавничо-поліграфічний центр «Київський університет», 2011. 208 с.
12. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein Introduction to Algorithms, Third Edition. Cambridge: MIT Press, 2009. 1320 p.

ІНФОРМАЦІЙНА БЕЗПЕКА ІНТЕРНЕТУ РЕЧЕЙ

Юскович-Жуковська В. І.
кандидат технічних наук, доцент,
доцент кафедри інформаційних систем та обчислювальних методів
Міжнародного економіко-гуманітарного університету
імені академіка Степана Дем'янчука
м. Рівне, Україна

В сучасному світі пристрої Інтернету речей (IoT) стають звичними інструментами буденних справ, а безпровідне, online та голосове керування ними за допомогою девайсів визначає новітній розвиток цифровізації.

Згідно досліджень компанії Juniper Research у 2022 році очікується активних IoT пристроїв у світі понад 50 мільярдів [1]. У доповіді Fortune Business зазначається, що світовий ринок Інтернету речей до 2026 року

досягне 1,11 трильйона доларів [2]. Ринок Інтернету речей розглядається аналітиками як найбільш перспективний у найближчому десятилітті [3].

В зв'язку із стрімким розвитком цифрових технологій, в тому числі технологій Інтернету речей, зростає кількість кібератак на популярні Інтернет-ресурси. Так, в результаті несанкціонованих втручань ставали недоступними web-сервіси Amazona, Twittera, GitHuba, Facebooka та інших соціальних мереж.

За даними досліджень корпорації HP безпечної системи Інтернету речей насьогодні не існує [1]. І пристрої IoT і їх мобільні та хмарні компоненти мають різноманітні вразливості. Кібератаки можуть призводити до неправильного поводження всієї інфраструктури IoT. Всі шлюзи, сервери та канали зв'язку, які забезпечують керування IoT, всі ПК та пристрої фактично є легкодоступними. Тому проблема інформаційної безпеки Інтернету речей є актуальною як для науковців, так і для компаній-розробників електронної техніки та програмного забезпечення.

Лідери IT-індустрії, провідні IT-компанії IBM, Intel, Cisco, Sumsung, General Electric, Google, Dell, AT&T, Національний інститут стандартів і технологій США, Консорціум індустріального Інтернету та ін. щорічно організовують міжнародні конференції з Інтернету речей – Всесвітній форум IoT (IoT World Forum, IWF), на якому різні IT-компанії представляють свої розроблені моделі захисту IoT. Так, компанія Cisco створила чотирьохрівневу архітектуру моделі безпеки розумних технологій та продемонструвала фреймворк на Всесвітньому форумі Інтернету речей [2].

Еталонна модель IoT для передачі зібраних даних використовує протоколи Bluetooth, NFC, RF, Wi-Fi, LoRaWAN і NB-IoT. Для забезпечення ефективного аналізу зібраної інформації, прийняття рішення та оперативного зворотнього зв'язку IT-компанії пропонують високотехнологічні IoT-платформи.

Так, розробка компанії Toshiba для інтеграції IoT-пристроїв і сервісів отримала назву Spinex. При розробці IoT-платформи Spinex використовувався досвід Toshiba в галузі інформаційних технологій, Інтернету речей, штучного інтелекту, розпізнавання голосу і відео, комп'ютерного зору.

Завдяки використанню відкритої архітектури Spinex може взаємодіяти з різними хмарними провайдерами та пристроями. Дана платформа надає користувачам три ключові переваги, які заключаються в наступному:

– всі базові операції виконуються в режимі реального часу, а обробку та аналіз зібраних даних виконують потужні сервери в хмарному середовищі;

– для побудови цифрових моделей реальних об'єктів використовується штучний інтелект, що дозволяє більш ефективно відслідковувати зміни обстановки та передавати пристроям необхідні команди;

– комп'ютерний зір та технологія аналізу відеоданих використовується для високоточної ідентифікації голосу та зображень.

У 2016 році Toshiba вже запустила заснований на Spinex хмарний сервіс IoT Standard Pack. Сервіс є уніфікованим рішенням для багатьох завдань, пов'язаних з Інтернетом речей. Він дозволяє швидко розгорнути мережу IoT в будь-якій організації за рахунок використання шаблонів для збору даних і швидкого підключення пристроїв до інфраструктури IoT з використанням технології plug-n-play. IWF прийняв еталонну модель IoT, як базову структуру і доповнив її до семи рівнів, включаючи інформаційну безпеку. Зважаючи на той факт, що ринок Інтернету речей ділиться на два великих сегменти: промисловий та споживчий, то вимоги до інформаційної безпеки IoT різняться.

Наявність вбудованого програмного забезпечення з функціями безпеки пристроїв, мережі та мобільних додатків для IoT запобігає проникненню потенційних кіберзагроз. Захист на рівні програмного забезпечення (ПЗ) включає авторизацію, аутентифікацію, конфіденційність, антивірусний захист тощо. Для безпеки промислового Інтернету речей виробники та постачальники IoT наділяють свої шлюзи ПЗ для захисту та керування пристроями та мережею. Для безпеки споживчого Інтернету речей користувачам варто в першу чергу замінити паролі на роутері, оскільки він є основним пристроєм IoT, а також зашифрувати веб-трафік. Базовим правилом кібербезпеки вважається регулярне оновлення функціоналу мобільних пристроїв, підключених до IoT. Широке застосування Інтернету речей має комплектуватися надійним ПЗ. Таким чином, для забезпечення захищеності інформації в системах IoT необхідно підходити комплексно, як апаратно, так і програмно.

Література:

1. Лобанчикова Н.М., Серденюк Б.О., Дослідження процесів захисту інформації в IoT. Режим доступу: https://conF. ztu.edu.ua/wp-content/uploads/2019/06/38-1.pdf
2. Що потрібно знати про Інтернет речей: фундаментальний лікбез. Режим доступу: https://www.telesphera.net/blog/iot-likbez.html
3. Гіоргізова-Гай В.Ш., Шеренковський А.О. Шлюз у системі Інтернету речей. Режим доступу: http://tech.vernadskyjournals.in.ua/journals/2019/1_2019/part_1/9.pdf