Секція 1

КРИПТОГРАФІЧНИЙ ЗАХИСТ IoT ПРИСТРОЇВ

Тяпко М. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В. Я.

Актуальність. Впродовж останніх років з розвитком технології Інтернет Речей (IoT) збільшується кількість пристроїв підключених до мережі Інтернет [1]. До пристроїв інтернет речей можна віднести розумні годинники, смарт-TV, пристрої голосового керування, камери, смарт-картки та інші. Деякі рішення зберігають та передають критично важливу інформацію. Для забезпечення конфіденційності та контролю цілісності даних використовується криптографія [2].

Метою даної роботи є дослідження існуючих рішень криптографічних алгоритмів для IoT девайсів.

Основні положення. Через те що більшість криптографічних алгоритмів було розроблено для використання серверами та звичайними комп'ютерами користувачів, багато з алгоритмів не підходять для пристроїв зі слабкими процесорами, низьким рівнем живленням та обмеженою пам'яттю, що є характеристиками пристроїв інтернет речей. Малоресурсна криптографія — це підгалузь криптографії, яка спрямована на надання рішень, розроблених для пристроїв із обмеженими можливостями [3], її мета полягає в розробці алгоритмів з низьким вмістом як апаратного, так і програмного забезпечення. Потреба оптимізації спонукає людей, що займаються криптографією, змінювати існуючі та створювати нові алгоритми. Таким чином з'явилися видозмінені версії AES, 3-DES, ГОСТ 28147-89, де були зменшені розміри блоку та відкритого ключу. Також з'явились нові шифри як Present, LEA, Simon, Speck та інші [4]. В 2015 році підрозділ Управління з технологій США National Institute of Standards and Technology (NIST) розпочав процес стандартизації та закликав компанії приєднатися до розробки криптографічних алгоритмів придатних для використання в обмежених середовищах [5]. Таким чином після завершення першого раунду відбору 32 із 56 запропонованих рішень було залишено для продовження розгляду, а після закінчення другого раунду в 2021 році після порівняння швидкості

шифрування та розміру коду алгоритмів залишилося лише 9 алгоритмів [5].

Висновки. Після порівняння результатів роботи алгоритмів та їх конфігурації можна зробити висновок, що AES не є універсальним рішенням тому що його апаратна реалізація має велике значення одиниці вимірювання Gate Equivalents (GE), ГОСТ 28147-89 займає менше місця, але може бути підвержений криптоаналізу. В тому числі, як і велика кількість нових шифрів, таких як SPECK, SIMON, через маленький розмір інформаційного блоку.

Список літератури

1. Internel of Thinks (IoT) market – growth, trends, COVID-19 impact and forecasts (2021-2026). *Mordon Intelligence*. URL – https://www.mordorintelligence.com/industry-reports/internet-of-things-moving-towards-a-smarter-tomorrow-market-industry (дата звернення: 18.11.2021);
2. Пєвнєв В.Я. Методи забезпечення цілосності інформації в інфокомунікаційних системах. Харків 2015 – с. 4. URL: http://repository.kpi.kharkov.ua/handle/KhPI-Press/19120 (дата звернення: 20.11.2021);
3. Report on Lightweight Cryptography, March 2017 – с. 1. *NIST*. URL – https://csrc.nist.gov/CSRC/media/Publications/nistir/8114/draft/documents/nistir_8114_draft.pdf (дата звернення: 19.11.2021);
4. An ultra light-weight cryptography scheme for IoT. *HAL*. URL – https://hal.archives-ouvertes.fr/hal-03359990/document (дата звернення: 18.11.2021);
5. Lightweigth Cryptography. *NIST*. URL – https://csrc.nist.gov/Projects/Lightweight-Cryptography (дата звернення: 18.11.2021).

Відомості про авторів

Тяпко Михайло Вікторович, бакалавр кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-494-57-95, m.tiapko@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu