DOI 10.6084/m9.figshare.22886720
*Виклики та проблеми сучасної науки, Том 1 (2023)*

# ПИТАННЯ ВИБОРУ ПЛАТФОРМИ РОЗРОБКИ IoT НА ОСНОВІ ВИМОГ МІЖНАРОДНИХ СТАНДАРТІВ З КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

*Валерій Борисович Мазуренко*
ORCID: https://orcid.org/0000-0001-8340-012X
Дніпровський національний університет імені Олеся Гончара, Дніпро

Інтернет речей (IoT – Internet of Things) безперервно збільшує свою присутність в нашому житті. Цьому процесу розширення в першу чергу сприяє зменшення вартості сенсорів, мікроконтролерів, приладів мережевої інфраструктури вкупі з активним розвитком різноманітних хмарних сервісів. Сьогодні самі звичайні люди мають доступ до технологій, які дозволяють збирати інформацію з різноманітних джерел, створювати автоматизацію для роботи побутової техніки та реалізовувати різноманітні сценарії взаємодії технічних об'єктів. Проте, як тільки користувач починає використовувати ці нові технології, відразу з'являється небезпека викрадання конфіденційних даних, підміни або знищення важливої інформації, появи спроб реалізації шкідливого функціювання системи та таке інше, – тобто всього того, що носить назву кібернетична загроза. Запобігти зазначеним загрозам можливо завдяки впровадженню в системах IoT стандартів з забезпечення кібернетичної безпеки.

Найбільш авторитетними організаціями, які створюють стандарти з кібербезпеки є наступні: ETSI (European Telecommunications Standards Institute) – Європейський інститут телекомунікаційних стандартів; IoTSF (Internet of Things Security Foundation) – Організація з безпеки інтернету речей; GSMA (Groupe Speciale Mobile Association) – Асоціація «Спеціальна група мобільних технологій»; NIST (National Institute of Standards and Technology) – Національний інститут стандартів і технології, США; IEEE (Institute of Electrical and Electronics Engineers) – Інститут інженерів з електротехніки та електроніки; IEC (International Electrotechnical Commission) – Міжнародна електротехнічна комісія; ENISA (European Union Agency for Network and Information Security) – Агентство Європейського Союзу з питань мережевої та інформаційної безпеки. Всі ці організації мають свої стандарти з кібернетичної безпеки IoT [1-3]. Зазначимо, що в першу чергу стандарти розрізняються за сферою застосування IoT, як то: промислова автоматизація, медицина, «розумний город», транспортні засоби, загальне призначення та таке інше. В цій роботі розглядається системи для потреб загального користування, таких наприклад, як «розумний будинок», тому доцільним було б спиратися на стандарт ETSI, який має назву «Кібербезпека Інтернету речей користувачів: основні

вимоги» [3]. Надалі в тексті будемо називати його просто «стандарт». Стандарт встановлює наступні основні положення забезпечення кібербезпеки інтернету речей.

1. Не використовуйте універсальних паролів за замовчуванням.
2. Впроваджуйте засоби керування звітами щодо вразливості.
3. Постійно оновлюйте програмне забезпечення.
4. Надійно зберігайте конфіденційні параметри безпеки.
5. Спілкуйтеся безпечно.
6. Зведіть до мінімуму відкритий простір для нападу.
7. Забезпечте цілісність програмного забезпечення.
8. Переконайтеся, що персональні дані захищені.
9. Зробіть системи стійкими до збоїв.
10. Перевіряйте дані системної телеметрії.
11. Спростіть для користувачів видалення даних користувачів.
12. Зробіть установку та обслуговування пристроїв простими.
13. Перевіряйте введені дані.

Частина цих вимог стосується апаратного та програмного забезпечення, яке використовується для створення системи IoT (мікроконтролера, його ОС та API), але не всі. Пункти 1, 6, 8, 9, 10, 11, 12, 13 – в першу чергу залежать від розробників та користувачів IoT. За належного програмування, вдалої конструкції та правильної експлуатації всі ці пункти можуть буть реалізовані практично на всіх популярних платформах. Звичайно, й всі інші пункти залежать від розробників та користувачів, проте їх не вдасться виконати, якщо мікроконтролер, операційна системи (ОС), прикладний програмний інтерфейс (API – Application Programming Interface) та підтримка виробника (у сукупності – платформа) не мають відповідних інструментів. Тому під час вибору платформи необхідно звертати увагу на те, якою мірою виробник мікроконтролера виконує вимоги пунктів 2, 3, 4, 5, 7. Коротко розглянемо зміст цих вимог. Почнемо з другого пункту стандарту. Стосовно засобів керування звітами щодо вразливості стандарт потребує відкритої публікації політики виробника щодо виявлення вразливостей. Це перша вимога з якої витікають усі наступні. Тому в процесі вибору платформи необхідно знайти ці звіти від компанії-виробника та оцінити періодичність їх появи.

Так само стосовно третього пункту основних вимог необхідно визначити, чи відбувається випуск оновленого програмного забезпечення на постійній основі. Оновлення операційної системи реального часу, якою виробник оснащує мікроконтролер має відбуватися не рідше, ніж раз на рік. Це є ознакою гарної практики. Мова йде про ядро системи, бібліотеки та засоби розробки програмного забезпечення. В кожної компанії-розробника може бути власна система представлення

оновлень, з якою обов'язково треба бути ознайомленим. Надійне збереження конфіденційних параметрів безпеки в мікроконтролері (пункт 4 вимог стандарту) забезпечується шифруванням файлової системи. Додатково може використовуватися шифрування енергонезалежної пам'яті. Якщо платформа не має таких опцій, то виконати пункт 4 буде неможливо. Пункт 5 вимог стандарту («безпечне спілкування») передбачає використання криптографічного захисту під час передавання даних. Задля виконання цього пункту найбільш зручним слід визнати наявність прикладного програмного інтерфейсу для роботи з TLS – криптографічним протоколом захисту на транспортному рівні (Transport Layer Security). В цьому випадку з'являються можливості для перевірки сертифіката сервера, автентифікації сертифіката клієнта та таке інше. На основі протоколу TLS реалізується протокол HTTPS, що дозволяє побудувати надійний зв'язок з хмарним сервером, так само, як й з IoT-пристроями. Стандарт вимагає (пункт 7) наявності засобів забезпечення цілісності програмного забезпечення шляхом застосування механізму безпечної загрузки, який передбачає використання цифрових підписів програмного коду. Важливо переконатися, що такий механізм існує.

Таким чином, реальний рівень безпеки системи IoT в першу чергу буде залежати від коректного вибору платформи розробника (мікроконтролер, ОС, API, підтримка) на основі вимог стандарту з кібербезпеки, чому треба приділити особливу увагу, а в решті решт – від якості розробки програмного забезпечення, вдалої конструкції пристроїв та правильної експлуатації – так само у відповідності до стандарту.

## Посилання

1. The IoT Security Assurance Framework Release 3.0 [Чинний від 2021-11]. IoT Security Foundation, 2021. 58 с. URL: https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf

2. NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline [Чинний від 2020-05]. National Institute of Standards and Technology, 2020. 23 с. URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR .8259A.pdf

3. ETSI EN 303 645 V2.1.1. CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements [Чинний від 2020-06]. ETSI, 2020. 34 с. URL: https://www.etsi.org/deliver/etsi_en/303600_303699 /303645/02.01.01_60/en_303645v020101p.pdf