Пановик Уляна Петрівна, *к.т.н., доцент,*
Українська академія друкарства, Львів

ВПРОВАДЖЕННЯ СТАНДАРТІВ ДЛЯ БЕЗПЕКИ СПОЖИВЧОГО ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей (IoT) – це нова сфера сучасних технологій, яка впливає на управління, освіту, бізнес, виробництво, транспорт, інфраструктуру, охорону здоров'я тощо. Створення узагальненої структури для IoT з різнорідними пристроями та технологічною підтримкою вимагає взаємодії між продуктами, програмами та послугами, що виключає прив'язку до постачальника. Крім того, темпи, з якими IoT розширюється, зараз прискорюються. Сьогодні, з появою 5G, Індустрії 4.0, а також зростанням використання та проникнення інтелектуальних пристроїв, мережева безпека стала важливою проблемою в епоху технологій, і багато пристроїв також починають демонструвати вразливості інформаційної безпеки, виникає проблема недостатнього захисту інформаційної безпеки. IoT – це, справді, цілісна концепція. Поєднання «розумних» пристроїв, мобільних або вебдодатків, які використовуються для взаємодії з ними, і хмарних сервісів, які дають змогу їм з'єднуватися один з одним, призводить до розвитку екосистем Інтернету речей. Однак разом зі збільшенням обсягу та функціональності підключених продуктів значно зростають ризики кібербезпеки, пов'язані із цими продуктами. Через обсяг цього ринку, а також його зв'язок з іншими середовищами високого ризику, це стає серйозною проблемою [1].

Для керування та перегляду інформаційної безпеки мережі можна застосувати IoT Security Foundation Framework, IEC 62443, вимоги OWASP IoT, вимоги GSMA IoT, серію UL 2900, ENISA Best Practices для підключених продуктів або ETSI EN 303 645.

ETSI EN 303 645 – це стандарт мережевої безпеки/захисту конфіденційності для споживчих продуктів IoT, який розроблений Технічним комітетом мережевої безпеки Європейського інституту стандартизації телекомунікацій (ETSI). Цей стандарт охоплює життєвий цикл продукту, безпеку програмного та апаратного забезпечення, захист конфіденційності та інші вимоги безпеки [2]. Усі продукти Інтернету речей, які продаються в ЄС, є обов'язковими для проходження перевірки інформаційної безпеки відповідно до директиви. ETSI EN 303 645 встановлює правила та вимоги щодо безпеки та конфіденційності пристроїв IoT, які охоплюють різні сфери та поділяються на такі категорії (рекомендації):

- безпека універсального пароля за замовчуванням;
- управління та виконання звітів про вразливості безпеки;
- оновлення програмного забезпечення;
- безпечне зберігання конфіденційних параметрів безпеки;
- безпека зв'язку;
- мінімізація поверхонь атаки;
- забезпечення безпеки персональних даних;
- забезпечення цілісності програмного забезпечення;
- стійкість системи до відключень;
- перевірка телеметричних даних системи;
- спрощення видалення даних користувача;
- полегшення встановлення та обслуговування обладнання;
- перевірка вхідних даних.

Наразі більшість пристроїв IoT на ринку відповідають лише трьом-чотирьом із зазначених рекомендацій. Однак, найпростішим способом відповідати мінімальним вимогам безпеки для пристроїв IoT був би обов'язковий стандарт і безумовна реалізація вимог безпеки.

Стандарт ETSI EN 303 645 був опублікований з основною ідеєю забезпечити більш чітке уявлення про реальні ризики та вразливості споживчих продуктів IoT, а також створити можливий підхід до тестування та оцінки. ETSI також розробляє методології для проведення валідаційного тестування відповідно до вимог ETSI EN 303 645. Програма сертифікації споживчого IoT має містити кілька аспектів, таких як: чіткі вимоги та методика тестування; плавний процес оцінювання та сертифікації, що призводить до обмежених зусиль; висока міжнародна видимість і визнання отриманого сертифіката. Наразі є кілька варіантів сертифікації, які є можливими для виробників: сертифікація Common Criteria, SESIP, лабораторія IoT Security Foundation або публічна та приватна сертифікація схеми, що працює на основі стандарту ETSI EN 303 645.

У цій множині доступних стандартів і варіантів сертифікації для виробників дуже важливо одержати найкраще рішення щодо конкретного стандарту або сертифікації, які вони будуть використовувати в процесі виробництва.

Список використаних джерел

1. Internet of Things, IoT. Technology Industry 4.0. IT-Enterprise. URL: https://it-enterprise.com/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot.
2. ETSI. Standards. URL: https://www.etsi.org/standards#Pre-defined%20Collections