УДК 004.738.5

СЕРТИФІКАЦІЯ КІБЕРБЕЗПЕКИ ІОТ: СИСТЕМА ТА СХЕМИ ОЦІНКИ ВІДПОВІДНОСТІ

Піхота К.В., Горицький В.М.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського
E-mail:pihotka19.11@gmail.com

IOT CYBER SECURITY CERTIFICATION: SYSTEM AND CONFORMITY ASSESSMENT SCHEMES

Cybersecurity certification of IoT components plays an important role in the field of cybersecurity. The creation of IoT cybersecurity certification systems and schemes on the basis of cross-border recognition is currently an urgent task for Ukraine. The report considers the main aspects of ensuring the recognition of the results of certification on the basis of international agreements of Ukraine on the recognition of the results of accreditation of conformity assessment bodies.

Важливу роль у сфері кібербезпеки відіграє сертифікація кібербезпеки компонентів IoT. Створення систем та схем сертифікації кібербезпеки IoT на засадах транскордонного визнання на сьогодні є актуальним завданням для України. В доповіді розглянуті основні аспекти забезпечення визнання результатів сертифікації на основі міжнародних угод України щодо визнання результатів акредитації органів з оцінки відповідності.

Кібербезпека інформаційних та комунікаційних технологій (далі – ІКТ) сьогодні визнана ключовою проблемою для збереження функціонування та безпеки цифрової економіки і державного управління в найближчому майбутньому [1, 2].

Важливу роль у сфері ІКТ відіграє оцінка відповідності (сертифікація) кібербезпеки ІКТ [3]. Це може відноситись до кібербезпеки компонентів, продуктів, обладнання, послуг та процесів ІКТ, до кібербезпеки хмарних сервісів, до кібербезпеки технологічних процесів, до особистої компетентності у сфері кібербезпеки тощо. Кібербезпека пристроїв IoT та механізмів їх використання у цьому переліку також займає важливе місце.

Правила, процедури та менеджмент проведення сертифікації кібербезпеки встановлюють схему сертифікації, а набір правил та процедур для управління подібними або спорідненими схемами оцінки відповідності утворюють систему сертифікації [4].

В статті розглядається важлива та актуальна для сьогодення України задача - розробка системи та схем сертифікації для (IoT) на основі існуючої в Україні системи технічного регулювання та досягнень в сфері оцінки відповідності та акредитації [5], а також вимог діючого законодавства України у сфері кібербезпеки, яке встановлює завдання на застосування кращих міжнародних та європейських принципів оцінки відповідності інформаційної та кібербезпеки [1].

Оцінка відповідності – це демонстрація того, що «зазначені вимоги» (specified requirement), які стосуються продукції, процесу, послуги, системи,

особи чи органу, були виконані (оцінка відповідності включає такі види діяльності, як випробування, інспектування, валідація, верифікація, сертифікація та акредитація). «Зазначена вимога» – потреба або сподівання, яке зазначено (ці вимоги можуть бути викладені в нормативних документах, таких як регламенти, стандарти та технічні специфікації). Об'єкт, до якого застосовуються ці «зазначені вимоги» є об'єктом оцінки відповідності. Схема оцінки відповідності – це набір правил та процедур, що описує об’єкти оцінки відповідності, визначає ці вимоги та забезпечує методологію проведення оцінки відповідності. Схемою з оцінки відповідності можна керувати в рамках системи оцінки відповідності. Система оцінки відповідності (conformity assessment system) – набір правил та процедур для управління подібними або спорідненими схемами оцінки відповідності. Оцінка відповідності встановленим вимогам неупередженою третьою стороною, яка називається органом з оцінки відповідності (ООВ), називається сертифікацією [4].

За останні десятиліття у світі була створена безліч систем та оціночних стандартів, які застосовуються для сертифікації інформаційної та кібербезпеки. Найбільш відомими серед них є: стандарти сімейства ISO/IEC 27000; стандарти сімейства IEC 62443; Framework v1.1 Національного інституту стандартів і технологій (NIST) США; стандарт COBIT-5; ISO/IEC 15408; ISO/IEC 18045:2008; FIPS - 140 – США та інші.

Практичне застосування названі системи та стандарти сертифікації знаходять здебільшого в галузевих схемах сертифікації. Таке різноманіття створює потужні технічні бар’єри у широкому чи транскордонному визнанні відповідних оцінок (сертифікатів). Крім того, у більшості випадків існування або використання різних вимог і процедур у тих секторах, які функціонують як глобальні і комплексні системи, може саме по собі являти собою підвищений ризик.

В роботі запропоновано створювати систему сертифікації кібербезпеки IoT на механізмах національної системи технічного регулювання, з опорою на міжнародні угоди Національного органу України з акредитації органів з оцінки відповідності та ієрархічній моделі оціночних стандартів Системи сертифікації кібербезпеки, запропонованій в [7].

У сучасному глобалізованому світі, з метою усунення технічних бар’єрів для визнання оцінок відповідності та сертифікатів, сформована глобальна система з оцінки відповідності, яка створює умови для взаємного визнання оцінок відповідності та сертифікатів. Ця система, – акредитація органів з оцінки відповідності (ООВ), до яких відносяться й органи з сертифікації [6].

У структурі технічного регулювання орган, відповідальний за акредитацію, оцінює компетенцію органів з сертифікації продукції, послуг та процесів, систем менеджменту, інспектування й персоналу, випробувальних й калібрувальних лабораторій. Офіційне визнання, іменоване акредитацією, засвідчує клієнтам і користувачам послуг компетентність діяльності даних організацій. Акредитація може забезпечити транскордонне визнання своїх послуг в рамках Міжнародного форуму з акредитації (IAF) і Міжнародного комітету з акредитації лабораторій (ILAC) [8,9].

IAF і ILAC сприяють й управляють визнанням Двосторонніх або Багатосторонніх Угод або Домовленостей (MRA/MLA), згідно з якими сторони, які беруть участь в них, погоджуються обопільно визнавати результати тестування, інспекцій, сертифікації або акредитації. Угоди MRA/MLA сьогодні стали важливим кроком на шляху оптимізації чи зменшення числа сертифікацій продуктів, послуг, систем, процесів і матеріалів, необхідних особливо в міжнародній діяльності [8,9].

На рисунку 1 представлено рівні та сфери, за якими в глобальній системі IAF визнано національний орган акредитації України.

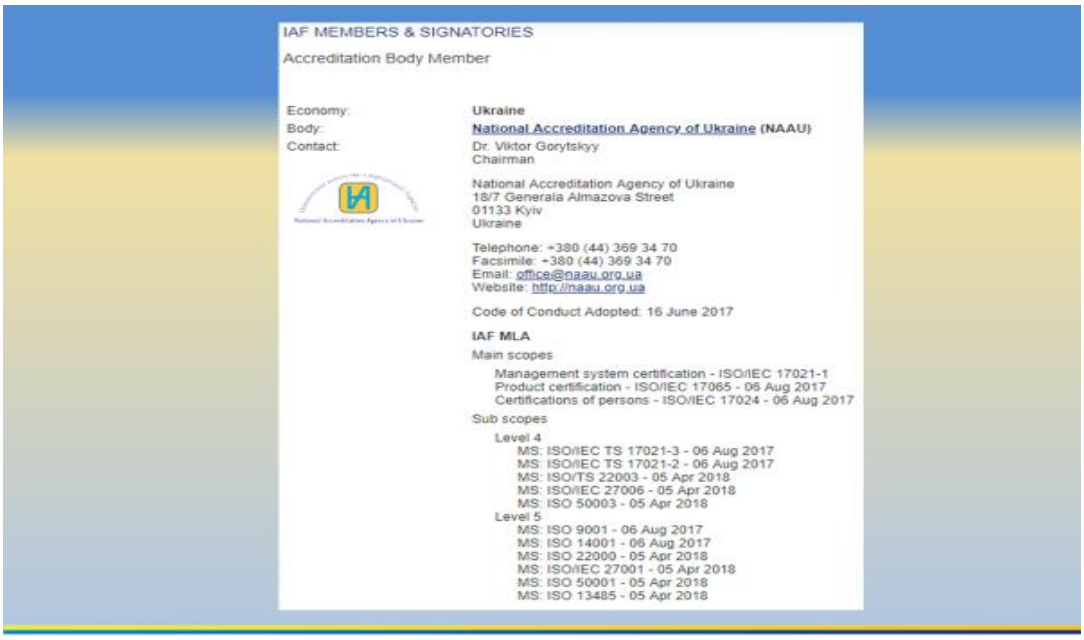

Рис. 1. Угода MRA та сфера в IAF.

Слід також додати, що глобальні системи IAF/ILAC діють через регіональні організації з акредитації, які входять до цих систем. Їх географічна локація зображена на рис. 2 та 3.

Для України регіональною організацією з акредитації є Європейська організація з акредитації (EA) [10].

Рис. 2. Регіональні організації ILAC.

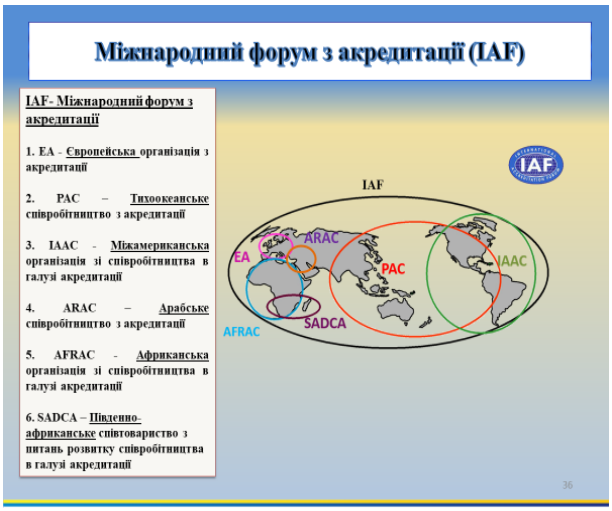

Рис. 3. Регіональні організації IAF.

Висновки.

Сертифікація кібербезпеки IoT потребує в цілях транскордонного визнання результатів сертифікації розробки відповідних схем та систем сертифікації.

Схеми сертифікації IoT в Україні можуть бути побудовані на механізмах національної системи технічного регулювання, з опорою на міжнародні угоди Національного органу України з акредитації органів з оцінки відповідності.

Література

1. Про основні засади забезпечення кібербезпеки України Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45.
2. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації Розпорядження Кабінету Міністрів України; від 17.01.2018 № 67-р. – Режим доступу : https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planu-zahodiv-shodo-yiyi-realizaciyi
3. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) – [Чинний від 2019-04-17]. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2019/881/oj.
4. Conformity assessment - Vocabulary and general principles : ISO/IEC 17000:2020. – [Чинний від 2020-01-06]. – International Organization for Standardization/International Electrotechnical Commission, 2020. – 30 P.
5. Про технічні регламенти та оцінку відповідності Закон України від 15.01.2015 № 124-VIII // Відомості Верховної Ради України. – 2015. – № 14.
6. Про акредитацію органів з оцінки відповідності Закон України від 17.05.2001 № 2407-III // Відомості Верховної Ради України. – 2001. – № 32.
7. Цвілій О.О. ІЄРАРХІЧНА МОДЕЛЬ ОЦІНОЧНИХ СТАНДАРТІВ СИСТЕМИ СЕРТИФІКАЦІЇ КІБЕРБЕЗПЕКИ ІКТ. DOI: 10.24412/9215-0365-2021-59-1-54-58. http://www.scientific-heritage.com/wp-content/uploads/2021/02/VOL-1-No-59-59-2021.pdf
8. International Accreditation Forum [Електронний ресурс]. – Режим доступу: https://www.iaf.nu/.
9. International Laboratory Accreditation Cooperation [Електронний ресурс]. – Режим доступу: https://ilac.org/.
10. European co-operation for Accreditation [Електронний ресурс]. – Режим доступу: https://european-accreditation.org/