УДК 006.3:004.738

СТАНДАРТИЗАЦІЯ ІНТЕРНЕТУ РЕЧЕЙ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У. П. Пановик

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Інтернет речей або IoT є новою галуззю сучасних технологій, яка має вплив на багато сфер нашого життя, зокрема бізнес, виробництво, розваги, транспорт, інфраструктуру, охорону здоров'я та багато інших. IoT передбачає взаємодію між різноманітними пристроями та технологічною підтримкою. Однак виклик для IoT полягає в створенні культури відкритості, яка забезпечить сумісність, підтримку багатьох програм та створення екосистем. У цьому контексті роль стандартів із чітко визначеними протоколами та сумісними інтерфейсами є ключовим фактором для забезпечення безперебійної роботи IoT. Глобальна стандартизація IoT є єдиним вирішенням цієї проблеми. Хоча вже є багато національних та міжнародних організацій зі стандартизації, проте є багато відкритих питань для обговорення, які потребують координації зусиль, розширення можливостей місцевих рішень та інших аспектів.

Проведено аналіз поточного стану стандартизації щодо нових підходів, які зараз застосовують організації зі стандартизації, і які швидко розширять сферу застосування поточних стандартів. Розглянуто взаємозв'язок між наявними стандартами IoT та проблемами, які потребують рішень. Окрему увагу приділено важливості стандартизації для України у контексті глобальних ініціатив, які мають підтримувати суспільний розвиток та економічне зростання.

Ключові слова: *Інтернет речей, стандартизація, пристрої, технології, інформаційна безпека, органи стандартизації.*

Постановка проблеми. Інтернет речей — одна з найпопулярніших концепцій у сучасному світі, яка з великою швидкістю втілюється в життя [3, 7].

Для реалізації IoT необхідна екосистема, яка містить «розумні речі» — різні пристрої, що оснащені датчиками; мережу доступу й передачі інформації; а також платформи для управління мережею, пристроями й додатками. Однак найбільшим аспектом є питання безпеки, після чого до 80 % інтелектуальних пристроїв є уразливими до зовнішніх атак. IoT схильний до таких ризиків: вразливість програмного забезпечення; незахищені канали зв'язку; витік інформації; шкідливі програми; кібератаки. Мають бути механізми для запобігання цих аспектів. Це передбачає написання стандартів і тестування обладнання, а також обов'язкове оновлення програмного забезпечення для вирішення проблем безпеки.

Пристрої IoT нині не мають універсальних стандартів і сертифікатів. А без цих надійних стандартів, яких мають дотримуватися виробники пристроїв та кінцеві

користувачі, Інтернет речей усе ще залишається досить уразливим. Стандартизація необхідна для забезпечення сумісності між пристроями, програмами та послугами, що унеможливлює прив'язку до постачальника; безпеки та конфіденційності даних і користувачів та взаємодії між фізичними системами зв'язку, синтаксисом протоколу, семантикою даних та інформацією домену.

Аналіз останніх досліджень та публікацій. Інтернет речей (IoT) впливає на нас у всіх сферах життя: робота, відпочинок, хобі, громадська діяльність тощо. Він змінює вплив на галузі, підприємства та суспільства [9, 11]. Для опису подібного явища використовуються такі поняття, як Інтернет реального світу (RWI), об'єкти, що підключені до Інтернету, Інтернет усього, Індустріальний Інтернет і Індустрія 4.0. Автор [8] стверджує, що є багато складнощів навколо Інтернету речей. Він визначає IoT як концепцію підключення будь-якого пристрою до Інтернету, що містить все, починаючи від мобільних телефонів, кавоварок, пральних машин, ламп, переносних пристроїв і майже всього іншого.

Окрім технологічних розробок у світі Інтернету речей, розглядаються і інші аспекти, наприклад, бізнес-екосистеми, що складаються з компаній, які надають пристрої з підтримкою Інтернету, програми, рішення для підключення та платформи для використання IoT [14]. Однак стандартизація поки що привертає менший інтерес дослідницьких спільнот. Технічна сторона IoT має певний розвиток у цьому плані, наприклад, упродовж останніх десятиліть різні органи стандартизації визначили декілька структур керування мережею.

У статті [6] зазначено, що суть цифрової еволюції полягає в тому, що дані з багатьох різноманітних джерел мають бути інтегровані та стандартизовані, щоб мати можливість аналізувати та одержувати з них сенс. Для цього потрібна певна стандартизація даних. Автор стверджує, що стандартизація відіграє важливу роль у тому, як швидко загальний підхід і промислові інтернет-технології будуть використані; які різновиди екосистем і платформ будуть; які бізнеси та домени першими адаптуються до зміни нової парадигми.

Як із наукового, так і з управлінського погляду питання стандартизації у сфері IoT є дуже складними. Автори публікації [4] стверджують, що в міру того як темпи розгортання IoT прискорюються, стандарти IoT зазнають серйозних змін. Концепція IoT дуже широка за своїм обсягом і охоплює майже всі аспекти життя. Унаслідок цього потенційна кількість стандартів дуже велика, а самі стандарти мають складну структуру. Крім того, технології постійно розвиваються, створюючи нові виклики.

Мета статті — виконати аналіз контенту з використанням концепції Інтернету речей; провести огляд стандартів, пов'язаних з IoT, окреслити сучасний стан стандартизації IoT та розглянути перспективи її розвитку.

Виклад основного матеріалу дослідження. Інтернет речей (Internet of Things, IoT) — це системи взаємопов'язаних між собою людей, фізичних об'єктів та IT-платформ, а також будь-яка технологія для кращої побудови, експлуатації та управління фізичним світом за допомогою повсюдного збору даних, інтелектуальних мереж, прогнозованої аналітики та глибокої оптимізації [5]. Спочатку

IoT-рішення були запроваджені для бізнесу та промисловості. Тепер «розумні» пристрої застосовують у будинках та офісах, намагаючись зробити доступними для всіх. IoT швидко розвивається в логістиці, аграрному секторі і розумних містах Smart City та скрізь, де є потреба в зборі даних і подальшому аналізі.

Основна ідея IoT полягає в контролі та моніторингу «речей» через обчислювальні пристрої, підключені через мережу з комутацією пакетів. Сьогодні IoT став новою парадигмою для Інтернету завдяки злиттю технологічних досягнень і легкої доступності пристроїв, що призвело до досі невивчених програм [10]. Для передачі даних пристроїв IoT застосовують такі різноманітні технології бездротового зв'язку, як IEEE 802.15.4, LoRaWan, LTE-M, Sigfox, NB-IoT, Bluetooth Low Energy (BLE), Wi-Fi, Z-Wave, ZigBee та інші комунікаційні технології, які мають свої особливості. Наприклад, Zigbee, BLE та WiFi мають обмежену дальність дії, тоді як 3G і LTE мають проблеми з енергоспоживанням та нестабільне покриття. Крім того, на сьогодні існує безліч платформ для розробки IoT-рішень, які надають різноманітні інструменти для розробки та керування мережею IoT.

Поширене підключення IoT-пристроїв створює приховані ризики для безпеки, а саме: прослуховування каналу бездротового зв'язку, несанкціонований доступ до пристроїв, втручання в роботу пристроїв і ризики конфіденційності. Можливість підключатися, керувати пристроєм і контролювати його з будь-якого місця та в будь-який час потребує відповідних заходів автентифікації та авторизації. Експерти з безпеки підкреслюють важливість безпеки в розгортанні IoT і попереджують про незахищеність поточних розгортань [2, 13]. Безпека для IoT охоплює широкий спектр завдань. Індивідуальні рішення безпеки, які пропонує спільнота IoT, пропонують переважно точкові рішення, але це мало допомагає зрозуміти загальну картину безпеки пристроїв IoT. Відповідно, посилена діяльність зі стандартизації для захисту IoT відіграє вирішальну роль у забезпеченні безпеки екосистеми IoT.

Для передачі даних від «розумних» пристроїв сьогодні є багато спеціалізованих стандартів. Міжнародні стандарти мають технологічні, економічні та суспільні переваги. Вони допомагають гармонізувати технічні характеристики продуктів і послуг, роблячи промисловість більш ефективною та руйнуючи бар'єри в міжнародній торгівлі. Стандарти також можуть бути офіційними і обов'язковими. Вони визначені офіційними організаціями стандартизації та можуть бути пов'язані з певним законодавством, і їх варто дотримуватися. Стандарти також можуть бути неофіційними, без офіційних рішень і зв'язків із законами та іншими офіційними правилами. Неофіційні стандарти можуть сформувати компанії або групи компаній, які першими вийшли на ринок або сферу застосування.

Практика показує, що стандартизація в галузі Інтернету речей усе ще розширюється. Є велика кількість організацій, які мають справу зі стандартами як офіційними, так і неофіційними, і простір їх застосування досить широкий. Багато нових програм використовують власні стандарти, і багато стандартів усе ще перебувають на стадії розробки. У стандартизації беруть участь альянси, консорціуми, регуляторні органи та органи стандартизації.

Органи стандартизації — це організації, що розробляють стандарти (Standards Development Organizations, SDO) або організації, що встановлюють стандарти (Standards-Setting Organizations, SSO), їх основною діяльністю є розробка, координація, перегляд і виготовлення технічних стандартів для задоволення потреб групи. Організації SDO можна розділити на два класи: загального та специфічного застосування. У першій категорії SDO, такі як ITU, IEEE, IETF, 3GPP і oneM2M, відіграють ключову роль у визначенні технологічних стандартів для охоплення загального простору проблем. Вони вказують або на політику, або на загальну еталонну архітектуру, або пропонують стандартний протокол для здійснення зв'язку. У другій категорії SDO створені в інтересах стандартизації технологій для певної сфери застосування. Ці SDO принципово використовують наявні архітектури та пропозиції протоколів із загальним підходом для створення моделі зв'язку. Вони створюють спеціальні стандарти для конкретних моделей обміну, щоб заповнити типові прогалини в доступних стандартних пропозиціях. Ці SDO зазвичай закриті в межах організацій-членів.

Оскільки IoT поширюється в різні галузі: від автономних транспортних засобів до точного землеробства, розумного виробництва, електронної охорони здоров'я та розумних міст, то і спектр стандартів, інструкцій, консорціумів і альянсів досить широкий, із великою кількістю варіантів. На рис. 1 наведено поточну ситуацію у світі IoT щодо стандартів і сфер застосування, у яких використовуються IoT.

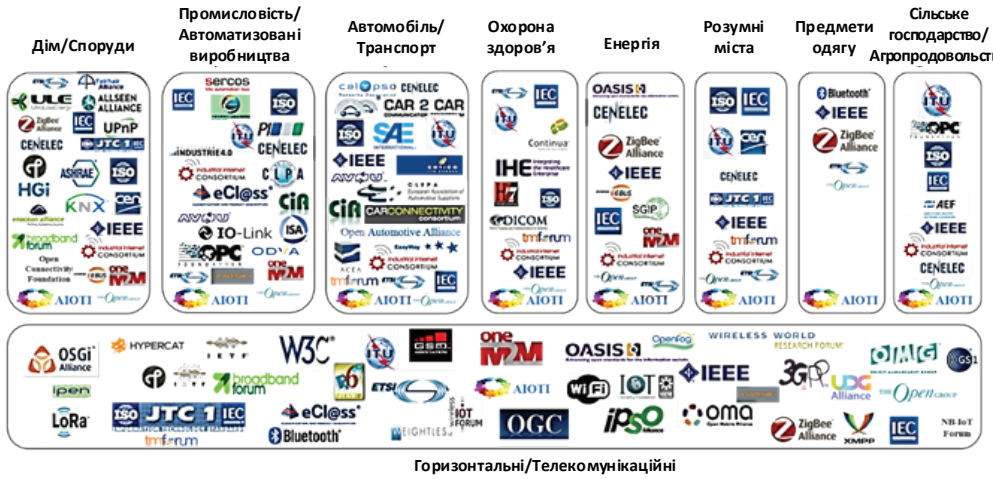

Рис. 1. Панорама органів стандартизації та альянсів IoT

Організації з розроблення стандартів є частиною альянсу AIOTI.

Альянс за інновації в Інтернеті речей (The Alliance for Internet of Things Innovation, AIOTI) запроваджений для створення та розвитку європейської екосистеми Інтернету речей, щоб прискорити її впровадження. У рамках цієї роботи AIOTI підтримує конвергенцію стандартів IoT, досліджує, як усунути перешкоди для впровадження IoT і погоджує діяльність ЄС з рештою світу в галузі Інтернету речей.

Ландшафт IoT, розроблений робочою групою AIOTI, використовує розрізнення між горизонтальними та вертикальними доменами (рис. 1) для класифікації організацій, які активно займаються стандартизацією IoT:

– вертикальні домени, які представляють 8 секторів, де розробляються та розгортаються системи IoT;
– горизонтальний рівень групує стандарти телекомунікацій, що охоплюють вертикальні домени й використовуються у всіх наведених сферах застосування.

У звіті [12] визначено 329 стандартів, які застосовуються до систем IoT. Ці стандарти були додатково класифіковані: 150 «горизонтальних» стандартів, які загалом стосуються зв'язку та підключення, інтеграції/сумісності та архітектури IoT; 179 «вертикальних» стандартів, які визначені у сферах розумної мобільності, розумного життя та виробництва. Панорама стандартизації IoT (рис. 1) чітко показує, що «горизонтальні» стандарти розробляють організації (SDO/SSO), які мають справу з IT-технологічними рішеннями. Потенціал «горизонтальних» стандартів матеріалізується, якщо розроблення стандартів IoT у вертикальних доменах буде ефективно використовувати ці стандарти.

Опишемо деякі з найбільших SDO/SSO, альянси та консорціуми, які прямо чи опосередковано зосереджені на стандартизації систем IoT.

Європейський інститут телекомунікаційних стандартів (The European Telecommunications Standards Institute, ETSI) зосереджує свою роботу в IoT на забезпеченні взаємосумісних і економічно ефективних рішень для M2M, особливо для інтелектуальних сервісів і програм для IoT. ETSI розробляє стандарти безпеки даних, керування даними, транспортування і обробки даних із конкретними ініціативами щодо інтелектуальних пристроїв, приладів, будинків, будівель, підключених транспортних засобів, розумних мереж і міст. ETSI співпрацює з oneM2M в IoT, наприклад, M2 TS 103 267SmartM2M; Розумна техніка; Комунікаційна структура; TS 103 264 SmartM2M; Довідкова онтологія та відображення oneM2M; TR 118 501 Колекція варіантів використання oneM2M; TR 103 290 Зв'язок між машинами (M2M); Вплив активності Smart City на середовище IoT; TR 118 506 Дослідження технологій забезпечення можливостей управління для розгляду oneM2M; TS 118 101 Функціональна архітектура.

Інститут інженерів з електротехніки та електроніки (The Institute of Electrical and Electronics Engineers, IEEE) має кілька груп, орієнтованих на IoT, зокрема ініціативну групу IEEE IoT та робочу групу IEEE P2413. Ініціатива група IoT розробляє стандарти і є центральною для всіх видів діяльності IEEE IoT. Робоча група IEEE P2413 зосереджується на розробленні еталонної архітектури IoT, що охоплює основні будівельні блоки, їхню можливість інтегрувати в багаторівневі системи та безпеку. IEEE P2413 розглядає IoT як просту трирівневу архітектуру з додатками, мережею та передачею даних, а також датчиками, які є важливими для зв'язку IoT. Сьогодні бездротова локальна мережа (сімейство IEEE 802.11) усе ще є практичним стандартом MAC для багатьох додатків IoT. Однак для роботи обмежених пристроїв із низьким енергоспоживанням у програмах Інтернету речей IEEE запропонував механізм доступу до персональної мережі малопотужних

сенсорних пристроїв із низькою швидкістю передачі. Технологія, стандартизована відповідно до IEEE 802.15.4, називається LowPAN. IEEE також докладає зусиль для визначення кількох технологічних стандартів, що охоплюють специфікації нижнього рівня, а також API рівня додатків у конкретних областях бездротового доступу в транспортному середовищі (WAVE), зв'язку на короткій відстані за допомогою видимого світла.

IEEE відіграє важливу роль у визначенні фізичного рівня та рівня каналу передачі даних, щоб забезпечити низький рівень сумісності між пристроями, а також у стандартизації механізмів безпеки, автентифікації та авторизації для рівня каналу даних, наприклад, IEEE P1912: Стандарт для архітектури конфіденційності та безпеки для споживчих бездротових пристроїв; IEEE 1451-99: Стандарт гармонізації та безпеки Інтернету речей; IEEE P2413: Стандарт архітектурної структури для IOT; IEEE 802.15.4-2015: Стандарт IEEE для низькошвидкісних бездротових мереж.

Сектор стандартизації телекомунікацій ITU (The ITU Telecommunication Standardization Sector, ITU-T) є одним із трьох філій Міжнародного союзу електрозв'язку (ITU). Він відповідає за координацію стандартів телекомунікацій та інформаційно-комунікаційних технологій. Його роботою керує Дослідницька група 20 (SG20), яка зосереджена на IoT та розумних містах і спільнотах. Його цілі містять вимоги до стандартизації для скоординованої розробки технологій IoT, таких як M2M і повсюдні сенсорні мережі, а також наскрізну архітектуру для IoT.

Союз ITU відповідає за Інтернет речей та його програми, включаючи аспекти семантики; аспекти великих даних; детальні вимоги до мереж, що підтримують програми IoT; аспекти обліку та нарахування; ідентифікацію, безпеку та конфіденційність; відкритість тощо. ITU також визначив еталонні архітектури для різних застосувань, включаючи інтелектуальне виробництво та промисловий IIoT, електронну охорону здоров'я та сільське господарство, переносні пристрої та послуги, кооперативні програми та послуги з безпеки транспортування тощо. Він використовує стандарти, створені відкритими SDO, такими як IETF та IEEE. Ключові стандарти, опубліковані ITU: X.509. Інфраструктура відкритих ключів (PKI); серії Y.3172, Y.3173, Y.3176, Y.3181. Машинне навчання для 5G і майбутніх мереж (IMT2020); серії H.263, H.264 (MPEG-4 AVC), H.265 (HEVC), H.266 (VVC). Кодування відео; серії JPEG T.8x, JPEG 2000 T.80x і JPEG XR T.83x. Кодування нерухомих зображень; ISDN і PSTN / 3G, H.320 і H.324. Системи відеоконференцій.

Інженерна робоча група Інтернету (The Internet Engineering Task Force, IETF) є провідною організацією зі стандартизації протоколів для Інтернету на різних рівнях мережевого стека. Вона має спеціальну групу IoT, яка координує діяльність, що пов'язана з IoT, в інших групах стандартів.

Останнім часом IETF бере активну участь у створенні спеціальних стандартів для широкого спектра технологій для IoT, відомих як LPWAN. Робоча група зосереджена на забезпеченні підключення IPv6 через наступний вибір малопотужних широкозонних технологій: SigFox, LoRa, 3GPP і NB-IOT. Метою таких ініціатив є пристосування наявних пропозицій IETF, щоб задовольнити конкретні вимоги

для забезпечення IP-сумісності певних технологій доступу. IETF є ключовим у визначенні функцій безпеки для майбутніх пристроїв IoT/M2M.

Перелік стандартів великий за обсягом. Можемо лише звернути увагу на такі стандарти IETF: RFC 7668: IPv6 через BLUETOOTH(R) Low Energy; RFC 7428: Передача пакетів IPv6 через мережі ITU-T G.9959; RFC 6550: RPL: Протокол маршрутизації IPv6 для мереж із низьким енергоспоживанням і мережами з втратами; RFC 7390: Груповий зв'язок для протоколу обмежених програм (CoAP); RFC 7744: Випадки використання для автентифікації та авторизації в обмежених середовищах; RFC 7554: Використання IEEE 802.15.4e перемикання каналів із часовими інтервалами (TSCH) в IoT: Постановка проблеми та інші.

Міжнародна електротехнічна комісія (The International Electrotechnical Commission, IEC) — міжнародна організація зі стандартизації у сфері електричних, електронних і суміжних технологій. Для забезпечення надійності та захищеності інформаційних систем IoT організація IEC запустила: стандарт IEC 62443 для кібербезпеки промислових систем керування, що є найпоширенішим стандартом промислової безпеки у всьому світі, особливо для IoT; стандарт IEC 62351 для безпеки даних і комунікацій в управлінні енергетичними системами разом із пов'язаним обміном інформацією.

Деякі зі стандартів IEC розробляються спільно з *Міжнародною організацією зі стандартизації* (International Organization for Standardization, ISO). Стандарти, створені спільно з ISO, позначаються ISO/IEC, а для їх спільної роботи в напрямі IoT-сфери створено робочу групу ISO/IEC JTC 1/SWG 5 при об'єднаному технічному комітеті ISO/IEC JTC 1.

ISO/IEC JTC 1/SWG 5 (Internet of Things, IoT) — це спеціальна робоча група (SWG) зі стандартизації ISO/IEC JTC 1, ISO та IEC), яка розробляє та сприяє розробленню стандартів для IoT. Метою ISO/IEC JTC 1/SWG 5 є не розробка або публікація стандартів, пов'язаних з IoT, а координація з робочими групами та спеціальними робочими групами ISO/IEC JTC 1, а також з іншими організаціями зі стандартизації, щоб допомогти краще визначити вимоги ринку та передати потреби і прогалини у світі щодо стандартизації для IoT. Група експертів представила стандарти, що допоможуть усвідомити потенціал IoT: ISO/IEC 30141: Інтернет речей (IoT): Еталонна архітектура; ISO/IEC 27400: Кібербезпека. Безпека та конфіденційність Інтернету речей: Керівні принципи; ISO/IEC 27402: Кібербезпека. Безпека та конфіденційність Інтернету речей: Базові вимоги до пристроїв; ISO/IEC 30149 ED1: Інтернет речей (IoT): Принципи надійності; ISO/IEC 30161-1 ED1: Інтернет речей (IoT): Платформа обміну даними для послуг IoT. Частина 1: Загальні вимоги та архітектура; ISO/IEC 30165: Інтернет речей (IoT): структура IoT у реальному часі; ISO/IEC 21823: Інтернет речей (IoT): Інтероперабельність систем IOT (Ч. 1. Структура; Ч. 2. Стандарт транспортної сумісності; Ч. 3. Стандарт семантичної сумісності).

Організація з удосконалення стандартів структурованої інформації (The Organization for the Advancement of Structured Information Standards, OASIS) займається розробленням, конвергенцією і ухваленням відкритих стандартів у рамках

міжнародної інформаційної спільноти. Окрім цього, консорціум сприяє галузевому консенсусу та виробляє стандарти безпеки, Інтернету речей, хмарних обчислень, енергетики, контентних технологій та керування надзвичайними ситуаціями. OASIS фінансують провідні IT-корпорації, такі як IBM, Novell, Oracle, Microsoft, Sun. Зокрема, IBM під егідою OASIS представила пару протоколів під назвою MQTT і MQTT для датчиків (MQTT-S), які призначені для роботи через TCP/IP. Протокол працює в режимі публікації/підписки для підключення пристроїв та покладається на рівень TCP для забезпечення надійності та безпеки. Деякі з найпоширеніших стандартів OASIS включають AMQP, CAP, CMIS, DITA, DocBook, KMIP, MQTT, OpenC2, OpenDocument, PKCS, SAML, STIX, TAXII, TOSCA, UBL і XLIFF. Багато з них були опубліковані як стандарти ISO, IEC або ITU.

oneM2M зосереджується на розробленні архітектури та стандартів зв'язку, а також на безпеці, сумісності та специфікаціях міжмашинних технологій для пристроїв і програм M2M/IoT. Стандартизовані специфікації, розроблені oneM2M, дають змогу екосистемі підтримувати широкий спектр програм і послуг, таких як розумні міста, розумні мережі, підключені автомобілі, домашня автоматизація, громадська безпека та охорона здоров'я.

oneM2M представив архітектуру сервісного рівня для всіх пристроїв M2M/IoT для безпроблемної взаємодії та обміну даними різних пристроїв IoT. Архітектура oneM2M використовує багаторівневий підхід, у якому кожен рівень відповідає за виконання певного набору функцій. Рівні містять програмний рівень, загальний рівень послуг та мережевий рівень. Також oneM2M надає специфікацію рівня обслуговування для служб M2M, щоб вони могли взаємодіяти та безперешкодно обмінюватися повідомленнями. Для обміну повідомленнями він покладається на мережу постачальників послуг. Будь-який примітив рівня обслуговування oneM2M можна відобразити через IP-мережу або інші мережі.

Він надає широкий набір інструкцій, формат адресації, API та зв'язки з найпопулярнішими протоколами IoT. Він також надає механізм для роботи пристроїв, що не є oneM2M, у мережі oneM2M. Це робить oneM2M унікальною платформою, яка забезпечує єдину структуру для обміну повідомленнями через різні пристрої та мережі. Стандарти oneM2M визнані на міжнародному рівні та транспоновані ITU-T у серії Y.4500.

Партнерський проєкт 3-го покоління (The 3rd Generation Partnership Project, 3GPP) — це проєкт, який об'єднує SDO з усього світу та був спочатку створений для розроблення технічних специфікацій для 3-го покоління мобільного стільникового зв'язку. Пізніше було запроваджено мобільний зв'язок 4-го покоління з LTE, а нещодавно — 5-го покоління (5G). Розроблені 3GPP технології містять EDGE, HSPA, агрегацію несучих, технології NR, EPC і NG-CN. Тобто 3GPP організовує свою роботу за трьома різними потоками: мережі радіодоступу, послуги та системні аспекти, а також базова мережа та термінали.

Основним напрямом 3GPP є передача невеликих даних із низьким енергоспоживанням. Загалом 3GPP об'єднує телекомунікаційні SDO для створення звітів і специфікацій для стільникового зв'язку через вузькосмуговий IoT (NB-IoT). Це

радіостандарт, який розроблений для малопотужної глобальної мережі (LPWAN) для підтримки технологій IoT. Результатом роботи 3GPP є розробка та підтримка: GSM і відповідні стандарти 2G і 2.5G, зокрема GPRS і EDGE; UMTS і відповідні стандарти 3G, зокрема HSPA та HSPA+; LTE і відповідні стандарти 4G, зокрема LTE Advanced і LTE Advanced Pro; 5G NR і відповідні стандарти 5G.

Як згадувалося раніше, є альянси та SDO з конкретним завданням заповнити певні прогалини, використовуючи стандартні пропозиції для конкретної технології. Одним із прикладів є *Fairhair Alliance*, який займається стандартизацією технологій керування освітленням та автоматизації будівель. Основні технології та протоколи базуються на загальних спеціальних пропозиціях IoT від IETF, IEEE, 3GPP тощо. *Fairhair* намагається заповнити конкретні технологічні прогалини (спеціальні процедури безпеки, типова підтримка багатоадресної передачі, ексклюзивна оптимізація рівня протоколу тощо), пов'язані з додатками у відповідній бізнес-сфері. Його роботою керують такі фахівці в галузі керування освітленням і автоматизації дому/будівель, як Philips, Seimens тощо. Іншим важливим учасником цього альянсу є *Thread Group*, яка керує мережевим протоколом IPv6 для IoT для автоматизації домашніх пристроїв, таких як освітлення та системи безпеки в локальній бездротовій мережі й значною мірою керується Google. Ці альянси усувають важливі прогалини в конкретних програмах для сумісності периферійних пристроїв у розумних будинках.

У міру того, як галузь розвивається, зростає потреба в стандартній моделі для виконання поширених завдань IoT, таких як обробка, зберігання та оновлення мікропрограми. У цій новій моделі різні рішення IoT мають працювати із загальними серверними службами, що гарантуватиме рівні сумісності, портативності та керованості, яких майже неможливо досягти за допомогою поточного покоління рішень IoT. Ця модель має подолати всі наявні перешкоди та виклики, які постають перед стандартизацією та впровадженням рішень IoT. Ці перешкоди можна розділити на чотири категорії (рис. 2).

Рис. 2. Компоненти стандартизації IoT

Категорія «платформа» передбачає форму та дизайн продуктів, інструменти аналітики, які використовуються для безпечного опрацювання величезного обсягу потоку даних з усіх продуктів, а також масштабованість, що означає широке застосування протоколів, таких як IPv6, у всіх вертикальних та горизонтальних ринках. На етапі підключення враховується взаємодія споживача з усіма аспектами їх повсякденного життя — від одягу, розумних автомобілів та розумних будинків до масштабних рішень для розумних міст. З погляду бізнесу — це підключення за допомогою IIoT (промислового Інтернету речей), де переважають комунікації M2M. Бізнес-модель стимулює до інвестування та управління будь-яким IoT-бізнесом. Необхідність надійної бізнес-моделі для IoT полягає в тому, щоб уникнути

повторення сценарію бульбашки. Ця модель має задовольняти всі вимоги для всіх видів електронної комерції, зокрема вертикальні, горизонтальні та споживчі ринки. Однак на цю категорію завжди впливає нормативно-правовий контроль. А от категорія «вбивчі програми» передбачає розвиток єдиної платформи IoT за допомогою додатків-вбивць, які містять контроль «речей», збір «даних» і аналіз «даних», що необхідні для створення вбивчих програм.

Усі чотири категорії взаємозалежні. Відсутність хоча б однієї з них може призвести до порушення моделі та зупинки процесу стандартизації. Розроблення такої моделі потребує великих зусиль. У кожній категорії залучено багато компаній, тому складно організувати спільну роботу для узгодження уніфікованої моделі.

Україна стикається зі своїми викликами в галузі Інтернету речей. На сьогодні цей сектор майже не захищений. Порівняно з розвиненими країнами, Україна має недоліки в нормативно-правовому забезпеченні цієї галузі. На цей час держава має деякі закони, які стосуються кібербезпеки, але жоден із них не охоплює повною мірою проблему кібербезпеки в новітньому цифровому середовищі. Деякі закони містять термін «Інтернет речей», але їхні норми не містять регулювання пристроїв IoT як окремої категорії. На законодавчому рівні варто розуміти, що будь-який пристрій, підключений до Інтернету, підпадає під відповідні закони. Якщо пристрій IoT використовується зловмисником для здійснення протизаконних дій, то власник цього пристрою може бути притягнутий до відповідальності. На жаль, не має законодавчих вимог до впровадження заходів безпеки з боку користувачів пристроїв IoT. Більшість користувачів не усвідомлюють наслідки можливих дій зловмисників і не володіють інструментами інформаційного захисту.

Питання стандартизації в галузі промислової автоматизації в Україні залишаються невирішеними. Деякі роботи здійснюються в рамках державно-приватного партнерства на рівнях Мінекономрозвитку України та Координаційної ради із цифрової економіки, яка є консультативно-дорадчим органом при міністерстві. Фахівці з Технічного комітету 185 (ТК 185) стверджують, що в Україні немає відповідної національної розробки в цій галузі, але є високоякісні міжнародні стандарти IEC, які потребують адаптації для використання в Україні. Експерти комітету наголошують на необхідності стандартизації, розробленні та прийнятті відповідних ДСТУ з термінології. На жаль, в Україні більшість національних стандартів відстають, порівняно з міжнародними стандартами. Більшість стандартів у сфері промислової автоматизації не застосовується або ігнорується, замовники здебільшого використовують стандарти, що датовані початком 90-х років минулого століття. Технічні комітети не досягають швидкої гармонізації стандартів через низьку інституційну спроможність. Легалізація міжнародних стандартів на рівень ДСТУ недостатня для їх прийняття ринком. Це призводить до ігнорування або поверхневого використання стандартів у технічних політиках підприємств. Промисловці та розробники мають низький рівень обізнаності в сучасних стандартах та розуміння їх ролі та впливу на технічні політики та на зростання конкурентоспроможності [1]. Хоча можна вказати на суттєвий прорив у напрямі впровадження стандартів в Україні. У 2019 році наказом ДП «УкрНДНЦ»

№ 249 були введені в дію національні стандарти, гармонізовані з європейськими та міжнародними стандартами: серія ДСТУ EN 61508:2019 (EN 61508:2010, IDT; IEC 61508:2010, IDT): Функційна безпечність електричних, електронних, програмованих електронних систем, пов'язаних із безпекою (Частина 1–7).

Висновки. Проведений аналіз стандартизації в усьому світі показує, що стандартизація в галузі IoT усе ще розширюється. Фігурує велика кількість організацій, які створюють стандарти, простір застосування яких досить широкий. Очевидно, що подальший розвиток і широке застосування IoT буде потребувати більш глибшої співпраці. Оскільки інтелектуальні речі пов'язані між собою, то інтерфейси між кінцевими пристроями мають бути визначені на технічному та прикладному рівнях, щоб одержати всі переваги IoT. Однією з найбільших проблем, від якої залежить кінцевий успіх IoT, є розроблення глобальних сумісних стандартів. Однак стандарти IoT сьогодні все ще широко відкриті — на рівні пристрою, протоколу та програмного забезпечення, оскільки не має глобальних валідованих рамок стандартизації. А досягнення повного потенціалу IoT буде значно ускладнене за відсутності відповідних стандартів та їх невиконанням.

Робота зі стандартизації IoT прогресує у багатьох напрямах. Також варто зазначити різноманітні поточні глобальні зусилля зі стандартизації і в Україні. Щоб IoT та життєво важливі мережі IoT були успішними в Україні, важливо визначити правильні варіанти використання разом із правильною політикою розгортання, зберігаючи водночас доступність технології для користувача. Потрібно, щоб Україна розширила свою участь у глобальному процесі стандартизації у сфері систем IoT, щоб врахувати варіанти використання та потреби українців.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ріст обізнаності та кращого використання міжнародних технічних стандартів в сфері промислової автоматизації України. Фінальний звіт за результатами проєкту aCampus ТК 185 Промислова автоматизація, 2020. URL: https://mautic.appau.org.ua/asset/134:acampus-final-report-21-02-02pdf.
2. Schneier Bruce. The internet of things is wildly insecure - and often unpatchable. *Wired*. 2014. URL: https://perma.cc/YT7P-2K25.
3. Dave Evans. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. *Cisco White Paper*. 2011. URL: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
4. Elloumi O., Song JS., Ghamri-Doudane Y., Leung V.C.M. IoT/M2M from Research to Standards: The Next Steps (Part II). Guest Editorial. IEEE Communications Magazine, Communications Standards Supplement, 10-11. 2015. DOI: 10.1109/MCOM.2015.7355578.
5. Internet of Things (IoT) Ecosystem Study. The Institute of Electrical and Electronics Engineers. Executive Summary. IEEE Standards Association, 2015. New York, USA. URL: https://iot.ieee.org/images/files/pdf/iot_ecosystem_exec_summary.pdf.
6. Larsen A. H. Life Science Digitalization – Standardization Is Core. 2016. URL: https://blogs.sas.com/content/hiddeninsights/2016/01/12/life-science-digitalization-standardization-is-core/.

7. More than 50 billion. connected devices. *Ericsson White Paper.* 2011. URL: https://vdna.be/publications/Wp-50-Billions.Pdf.
8. Morgan J. A Simple Explanation Of «The Internet Of Things». *Forbes.* May 13, 2014. URL: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=4d127b0e1d09.
9. Muhonen T. Standardization of Industrial internet and IoT (IoT – Internet of Things) – Perspective on condition-based maintenance. *Master's thesis. University of Oulu.* 2015.
10. Rose K., Eldridge S., Chapin L. The Internet of Things: An Overview, Internet Society Document, 2015. URL: https://api.semanticscholar.org/CorpusID:9217381.
11. Ranger Steve. What is the IoT? Everything you need to know about the Internet of Things right now. 2020. URL: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.
12. STF 505 TR 103 375. SmartM2M IoT Standards landscape and future evolution, 2016. URL: https://docbox.etsi.org/SmartM2M/Open/AIOTI/STF505.
13. Strategic principles for securing the internet of things (IoT). U.S. Department of Homeland Security, Version 1.0. 2016. URL: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf.
14. Toivanen T., Mazhelis O., Luoma E. Network Analysis of Platform Ecosystems: The Case of Internet of Things Ecosystem. *Software Business. Springer International Publishing.* 2015. 30-44. DOI:10.1007/978-3-319-19593-3_3.

REFERENCES

1. Rist obiznanosti ta krashchoho vykorystannia mizhnarodnykh tekhnichnykh standartiv v sferi promyslovoi avtomatyzatsii Ukrainy. Finalnyi zvit za rezultatamy proiektu aSampus TK 185 Promyslova avtomatyzatsiia, 2020. Retrieved from https://mautic.appau.org.ua/asset/134:acampus-final-report-21-02-02pdf (in Ukrainian).
2. Schneier, Bruce. (2014). The internet of things is wildly insecure - and often unpatchable. Wired. Retrieved from https://perma.cc/YT7P-2K25 (in English).
3. Dave, Evans. (2011). The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Cisco White Paper. Retrieved from http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (in English).
4. Elloumi, O., Song, JS., Ghamri-Doudane, Y., & Leung, V.C.M. (2015). IoT/M2M from Research to Standards: The Next Steps (Part II). Guest Editorial. IEEE Communications Magazine, Communications Standards Supplement, 10-11. DOI: 10.1109/MCOM.2015.7355578 (in English).
5. Internet of Things (IoT) Ecosystem Study. The Institute of Electrical and Electronics Engineers. Executive Summary. IEEE Standards Association, 2015. New York, USA. Retrieved from https://iot.ieee.org/images/files/pdf/iot_ecosystem_exec_summary.pdf (in English).
6. Larsen, A. H. (2016). Life Science Digitalization – Standardization Is Core. Retrieved from https://blogs.sas.com/content/hiddeninsights/2016/01/12/life-science-digitalization-standardization-is-core/ (in English).
7. More than 50 billion connected devices. (2011). Ericsson White Paper. Retrieved from https://vdna.be/publications/Wp-50-Billions.Pdf (in English).

8. Morgan, J. (May 13, 2014.) A Simple Explanation Of «The Internet Of Things». Forbes. Retrieved from https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=4d127b0e1d09 (in English).
9. Muhonen, T. (2015). Standardization of Industrial internet and IoT (IoT – Internet of Things) – Perspective on condition-based maintenance. Master's thesis. University of Oulu (in English).
10. Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An Overview, Internet Society Document. Retrieved from https://api.semanticscholar.org/CorpusID:9217381 (in English).
11. Ranger, Steve. (2020). What is the IoT? Everything you need to know about the Internet of Things right now. Retrieved from https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ (in English).
12. STF 505 TR 103 375. SmartM2M IoT Standards landscape and future evolution. (2016). Retrieved from https://docbox.etsi.org/SmartM2M/Open/AIOTI/STF505 (in English).
13. Strategic principles for securing the internet of things (IoT) (2016). U.S. Department of Homeland Security, Version 1.0. Retrieved from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf (in English).
14. Toivanen, T., Mazhelis, O., & Luoma, E. (2015). Network Analysis of Platform Ecosystems: The Case of Internet of Things Ecosystem. Software Business. Springer International Publishing, 30-44. DOI: 10.1007/978-3-319-19593-3_3 (in English).

doi: 10.32403/0554-4866-2023-1-85-51-64

STANDARDIZATION OF THE INTERNET OF THINGS: CURRENT STATE AND DEVELOPMENT PROSPECTS

U. P. Panovyk

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine
ulianapanovuk@gmail.com

The Internet of Things (IoT) is now more than a new technology, and the IoT community has begun to develop ambitious solutions and deploy large and complex IoT systems. It affects many areas of our lives, including governance, education, business, manufacturing, entertainment, transportation, infrastructure, healthcare, and many others. The IoT involves interaction between various devices and technological support. This new IoT challenge will only be solved if the IoT community develops a culture of openness about interoperability, supporting numerous applications, and building healthy ecosystems. The role of standards is now widely recognized as one of the key drivers of this open approach, which requires common standards with well-defined protocols and interoperable interfaces to ensure seamless IoT operation. Global IoT standardization is the only solution to this problem.

A number of standards already exist for those developing IoT systems. They make it possible to meet many requirements of IoT systems in a wide range of solutions (from consumer to industrial) for numerous domains such as cities, eHealth, HR, transportation, etc. There are numerous organizations dealing with standards, both formal and informal, and the scope is wide. Many developing applications use their own standards, and many standards are still under development. Solutions rely on various coexisting protocols, interfaces, and platforms, either proprietary or off-the-shelf. Some IoT standards are formal standards, while some are informal standards agreed upon in forums or alliances or dictated by companies that play a critical role. Cooperation between different organizations is important and necessary. However, there are many open issues for discussion and standardization, which require coordination of efforts, empowerment of local solutions, and other aspects. The article analyzes the current state of standardization, particularly the new approaches currently being used by standardization organizations that will rapidly expand the scope of current standards. The relationship between the existing IoT standards and the problems that need solutions are considered. The importance of standardization for specific countries, in particular for Ukraine, in the context of global initiatives that support social development and economic growth, is noted.

Keywords: *Internet of things, standardization, devices, technologies, information security, Standards Development Organizations.*

Стаття надійшла до редакції 01.04.2023.
Received 01.04.2023.