https://orcid.org/0000-0002-9639-3544

УДК 004.457

О.Є. КОВАЛЕНКО[*, **]

МОДЕЛІ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

[*]Національний університет біоресурсів і природокористування України, м. Київ, Україна
[**]Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

Анотація. *IoT – це кіберконвергентна система, яка включає речі, засоби зв'язку, цільові програми та інструменти аналізу даних, які підтримують унікальну ідентифікацію кожного об'єкта. Технології IoT відіграють життєво важливу роль при створенні кіберконвергентних систем завдяки її широкому застосуванню в різних сферах життя, таких як промисловість, соціальна сфера, охорона здоров'я та створення комфортного середовища. Метою моделі безпеки IoT є забезпечення конфіденційності, цілісності та доступності даних, що передаються між пристроями, а також забезпечення конфіденційності та безпеки кінцевих користувачів. Створення та використання систем IoT безпосередньо впливає на безпеку та конфіденційність усіх залучених та пов'язаних компонентів. Представлене дослідження – це представляє аналіз моделей архітектури IoT із підтримкою наскрізної безпеки. Проведений огляд літератури розкриває проблеми різних аспектів безпеки, з якими стикається середовище IoT. Описані моделі, що реалізують різні стратегії безпеки на різних рівнях IoT, включають рівень сприйняття, який забезпечує процес автентифікації для ідентифікації об'єктів IoT, мережевий рівень, який фокусується на процесах безпеки хмарних платформ, та рівень застосунків, який забезпечує автентифікацію та авторизацію для кінцевих користувачів. Результати аналізу показують, що побудова безпечних систем IoT ґрунтується на трьох основних стратегіях: належному налаштуванні та забезпеченні захищеності всіх пристроїв IoT, використанні безпечних бездротових мереж для підключення пристроїв IoT до корпоративних або глобальних мереж, постійній ситуаційній обізнаності стосовно загроз безпеці пристроям IoT і впровадженні відповідних рішень безпеки для захисту їх від атак. Також описана модель зрілості безпеки систем IoT на основі пакета документів ISA/IEC 62443.*
Ключові слова: *інтернет речей, кіберконвергентна система, модель безпеки.*

Abstract. *The IoT is a cyber-convergent system that includes things, means of communication, target applications, and data analysis tools that support the unique identification of each object. IoT technologies play a vital role in the creation of cyber-convergent systems due to their wide usage in various spheres of life such as industry, social sphere, health care, and creating a comfortable environment. The IoT security model method ensures the confidentiality, integrity, and availability of data that is transferred between devices and also guarantees the privacy and security of end users. The creation and use of IoT systems directly affect the security and privacy of the involved and connected components. The presented study introduces an analysis of IoT architecture models with end-to-end security support. The conducted literature review reveals the challenges of various aspects of security faced by the IoT environment. Some models implementing different security strategies at different layers of the IoT are described. These include the perception layer which provides the authentication process for identifying IoT entities, the network layer which focuses on the security processes of cloud platforms, and the application layer which provides authentication and authorization for end users. The results of the analysis show that building secure IoT systems is based on three main strategies: proper configuring and ensuring the protection of all IoT devices; using secure wireless networks to connect IoT devices to corporate or global networks; constant situational awareness of security threats to IoT devices; and implementing appropriate security solutions to protect them from attacks. The maturity model of the IoT security system based on the ISA/IEC 62443 document package is also described.*
Keywords: *Internet of Things, cyber-convergent system, security model.*

DOI: 10.34121/1028-9763-2023-4-43-50

1. Вступ

Інтернет речей (IoT) є необхідною частиною сучасних комп'ютеризованих систем у різних сферах людської діяльності. IoT – це концепція комп'ютерної мережі фізичних об'єктів (речей), оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем, яка розглядає організацію таких мереж як явище, здатне змінити економічні та соціальні процеси, що усуває необхідність участі людини в частині дій і операцій. Загалом технології IoT збирають, обмінюються та обробляють дані з метою динамічної адаптації до певного контексту, трансформуючи діловий світ і спосіб нашого життя в цілому [1].

Загальні і спеціальні поняття і визначення IoT представлені у стандарті ISO/IEC 20924:2021. Цей ISO визначає IoT як «інфраструктуру взаємопов'язаних об'єктів, людей, систем та інформаційних ресурсів разом з інтелектуальними службами, що дозволяє їм обробляти інформацію фізичного та віртуального світу та реагувати». [2]. Рекомендація ITU-T Y.2060 зазначає, що «з точки зору технічної стандартизації IoT можна розглядати як глобальну інфраструктуру для інформаційного суспільства, що забезпечує передові послуги шляхом взаємозв'язку (фізичних і віртуальних) речей на основі існуючої та розвиваючої сумісної інформації та комунікаційні технології (ІКТ)» [3]. IoT – це кіберконвергентна система [4, 5], яка включає речі, засоби зв'язку, цільові програми та інструменти аналізу даних, які підтримують унікальну ідентифікацію кожного об'єкта. Кіберконвергентна система – це поєднання кібератичних систем і кібероб'єктів різного призначення для забезпечення функціонування цільових об'єктів у кіберзв'язаних світах.

Кібератика є цілісною галуззю досліджень для систематичного вивчення кібер-суб'єктів у кіберпросторі, їхніх властивостей і функцій, а також їхніх зв'язків і відносин з об'єктами у фізичному, соціальному та ментальному просторі. Для кібератики характерне не тільки відтворення людського інтелекту (наприклад, розумне відчуття, прийняття рішень і управління тощо), але й запозичення природних властивостей, наприклад, динаміки, самоадаптації, енергозбереження [6].

Зростаючий масштаб і складність систем IoT, з одного боку, і загрози безпеці, з іншого, вимагають розробки моделей та інструментів управління безпекою з урахуванням специфіки сфери використання.

Метою дослідження є аналіз моделей безпеки Інтернету речей для формулювання загальних підходів при практичному застосуванні в різних сферах діяльності.

2. Проблеми безпеки Інтернету речей

З поширенням застосування Інтернету речей зростають і ризики кібератак, направлених на різні рівні та компоненти Інтернету речей. IoT є точкою входу в організацію, на яку націлені кіберзловмисники з метою вчинення шкідливих дій: прослуховування, викрадення інформації, порушення операційної діяльності, виведення з ладу обладнання тощо.

Сучасні рішення безпеки, доступні для захисту систем із використанням IoT, ставлять виробників і операторів у складне становище. Як правило, такі рішення орієнтовані на периферійні області IoT і стримують кібератаки та загрози лише після їх ідентифікації. Визначають різні проблеми безпеки систем IoT, зокрема:

– відсутність стандартизації;
– слабка або відсутня автентифікація;
– неадекватна безпека програмного забезпечення;
– недостатня безпека мережі;
– обмежена фізична безпека;
– неналежний захист даних;

– обмежений захист конфіденційності;
– неможливість оновити або виправити пристрої;
– обмежений регулятивний нагляд;
– відсутність видимості та контролю;
– складнощі у виявленні загроз і реагуванні на них;
– реактивний підхід до загроз;
– неможливість постійного спостереження за пристроями;
– вразливість засобів IoT сторонніх розробників;
– застарілі засоби та методи безпеки;
– відсутність підходу до підвищення рівня безпеки;
– складність балансування між безпекою та продуктивністю.

Питання організації безпеки IoT розглядаються у великій кількості публікацій у цій галузі досліджень та інженерії з різних точок зору. Зокрема, загальні питання безпеки IoT розглядаються в [7, 8]. Безпека IoT з акцентом на вплив нових технологій представлена у роботі [9]. Питання формування вимог безпеки до компонентів IoT розглядаються в [10, 11]. Огляд заходів безпеки для IoT представлено в [12]. Окреме місце в дослідженнях із забезпечення безпеки IoT займають роботи, орієнтовані на використання формалізованих знань та онтологій [13–16].

2. Загрози безпеці систем Інтернету речей

Швидке зростання кількості підключених кінцевих точок IoT у різних галузевих сегментах і типах пристроїв сприяло повсюдному підключенню, периферійним обчисленням і доступності надійної хмарної основи для виконання робочих навантажень додатків на основі даних. Кількість атак на системи IoT збільшується пропорційно зростанню їх розмірів та складності.

Ризики безпеки системам IoT часто пов’язані з:

– порушенням безпеки транспортних засобів, пов’язаних із ризиками зламу, що відбуваються без відома водія;

– втручанням у роботу пристроїв IoT. Одним із найпоширеніших способів використання пристроїв IoT є втручання в їх мікропрограму, що може призвести до втрати або пошкодження даних;

– крадіжкою даних. Іншою поширеною загрозою безпеці Інтернету речей є крадіжка даних, яка часто робиться для отримання доступу до фінансової чи особистої інформації;

– незахищеністю підключення до Інтернету: відсутність стандартів безпеки може зробити пристрої IoT відкритими для атак і це також може включати хакерські атаки.

– уразливостями мікропрограмного забезпечення IoT із відкритим вихідним кодом. Багато пристроїв IoT створено з мікропрограмним забезпеченням із відкритим кодом, яке може бути вразливим до атак.

Приклад класифікації загроз безпеці IoT наведено на рис. 1 [17].

Немає єдиного рішення, яке могло б захистити всі пристрої IoT від усіх типів загроз, але є кілька загальних стратегій, які можуть допомогти зменшити ризики, створені цими пристроями.

Перша стратегія ґрунтується на належному налаштуванні та забезпеченні захищеності всіх пристроїв IoT. У рамках реалізації цієї стратегії передбачається налаштування облікових записів користувачів і паролів, брандмауерів і антивірусного програмного забезпечення, а також регулярні встановлення оновлень безпеки.

Друга стратегія полягає у використанні безпечних бездротових мереж для підключення пристроїв IoT до корпоративних або глобальних мереж. Це допомагає захистити

системи від атак і гарантує, що конфіденційні дані не передаються через незахищені мережі.

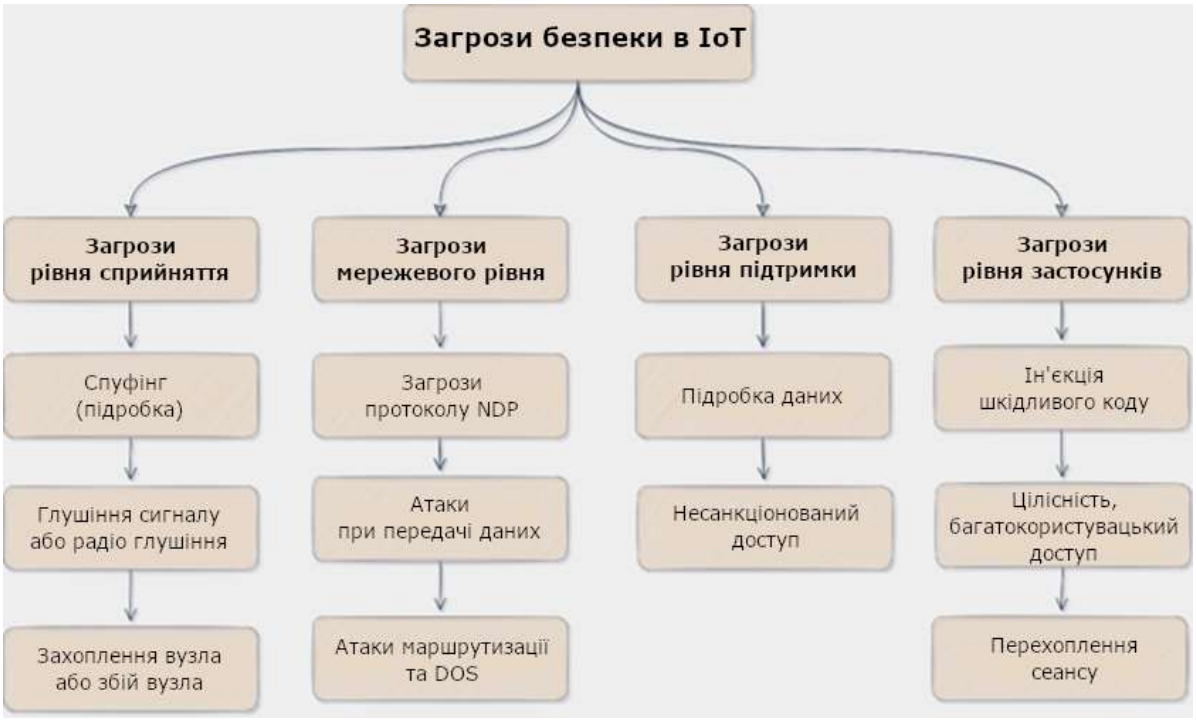

Рисунок 1 – Класифікація загроз системам IoT

Третя стратегія ґрунтується на постійній ситуаційній обізнаності стосовно загроз безпеці пристроям IoT і впровадженні відповідних рішень безпеки для захисту їх від атак. Це гарантує, що пристрої правильно налаштовані та захищені від атак, а особиста інформація не буде порушена.

3. Моделі безпеки Інтернету речей

Існують різні еталонні моделі IoT, запропоновані різними розробниками, зокрема, ENISA [1], ISO/IEC [2], ITU-T [3], Cisco, Intel, IBM [18] та ін. Питання безпеки є частиною цих еталонних моделей. Такі моделі забезпечують формальну структуру для реалізації безпеки та оцінки зрілості цих реалізацій. Модель безпеки IoT відноситься до набору заходів безпеки та протоколів, які захищають пристрої, мережі та системи від кібератак і порушень даних. Метою моделі безпеки IoT є забезпечення конфіденційності, цілісності та доступності даних, що передаються між пристроями, а також забезпечення конфіденційності і безпеки кінцевих користувачів.

При побудові моделей безпеки IoT використовують два підходи:

1) реалізація у багаторівневій архітектурі рівня безпеки, який охоплює весь стек від рівня комунікацій у граничній області IoT до рівня аналітичних застосунків;

2) наскрізна реалізація рішень безпеки в усіх точках, від граничних пристроїв через мережі та інтеграційні платформи до аналітичних застосунків.

Модель безпеки IoT стикається з кількома проблемами, що можуть вплинути на її ефективність у захисті пристроїв IoT і даних, які вони збирають і передають. Деякі з цих проблем перелічені нижче.

Складність: пристрої IoT стають дедалі складнішими, із зростаючою кількістю компонентів і систем, які необхідно захищати. Ця складність ускладнює впровадження комплексного рішення безпеки, яке може ефективно захистити всі аспекти системи IoT.

Неадекватні заходи безпеки: багато пристроїв IoT потребують більш адекватних заходів безпеки, таких як шифрування, брандмауери та системи виявлення вторгнень. Це робить такі пристрої вразливими для атак і використання зловмисниками.

Застаріле програмне забезпечення: багато пристроїв IoT працюють із застарілим програмним забезпеченням, яке виробник більше не підтримує. Це ускладнює застосування оновлень безпеки або виправлень для таких пристроїв, роблячи їх уразливими для атак.

Обмежена обчислювальна потужність: багато пристроїв IoT мають обмежену обчислювальну потужність, пам'ять і ємність для зберігання, що ускладнює запуск традиційного програмного забезпечення безпеки на них. Це робить такі пристрої вразливими для атак, оскільки зловмисники можуть використовувати відомі вразливості в цих пристроях, щоб отримати доступ до конфіденційних даних або контролювати пристрій.

Погано розроблені протоколи: протоколи, які використовуються для зв'язку між пристроями IoT та Інтернетом, можуть бути погано розроблені, що робить їх вразливими для використання. Наприклад, деякі протоколи можуть використовувати незашифрований зв'язок, що полегшує зловмисникам перехоплення та маніпулювання даними, які передаються.

Відсутність видимості: моніторинг і керування безпекою пристроїв IoT може бути складним, оскільки вони часто розгортаються у віддалених або недоступних місцях. Це ускладнює оперативне виявлення загроз безпеці та реагування на них.

Поведінка користувачів: безпека пристроїв IoT також залежить від поведінки користувачів. Наприклад, користувачі можуть використовувати слабкі паролі, нехтувати оновленнями програмного забезпечення або необережно поводитися з даними, якими вони діляться в Інтернеті, піддаючи свої пристрої та дані ризику.

Інтероперабельність: оскільки кількість пристроїв IoT продовжує зростати, існує потреба у взаємодії між ними, що може ускладнити впровадження узгодженого підходу до безпеки в усій екосистемі IoT.

Відсутність стандартів безпеки: екосистема IoT складається з величезної кількості пристроїв різних виробників, кожен зі своїми стандартами безпеки. Це ускладнює єдиний підхід до безпеки для всієї системи.

Погане тестування: більшість розробників IoT не надають пріоритету безпеці та проводять ефективне тестування уразливостей, щоб виявити слабкі місця в системах IoT.

Для кожного середовища IoT необхідно провести оцінку ризиків, щоб проаналізувати загрози, які можуть вплинути на різні активи, визначити вірогідні сценарії атак і помістити їх у контекст визначеної послуги IoT, визначивши, які небезпеки є критичними чи ні та які можна пом'якшити.

4. Модель зрілості безпеки Інтернету речей

Пакет документів Industry IoT Consortium (IIC) IoT Security Maturity Model (SMM) [19], що складається з Посібника для практиків, профільних документів і вказівок щодо відображення, надає детальну модель і підхід для досягнення належного рівня управління безпекою, технології та операційної зрілості для задоволення потреби бізнесу. Його можна використовувати в поєднанні з іншими детальними інструкціями, такими як IIC Industrial Internet Reference Architecture, IIC Industrial Internet of Things Connectivity Framework, IIC Industrial Internet of Things Security Framework, а також документ IIC Industrial Internet of Things Trustworthiness Framework як набір документації ISA/IEC 62443.

Пакет документів ISA/IEC 62443 [19], розроблений Міжнародним товариством автоматизації (ISA) та його комітетом ISA99, є апробованим, зрозумілим і прийнятим набором рекомендацій, який використовується в різних галузях, включаючи виробництво, комунальні послуги, зокрема, такі як електроенергія, вода, газові, транспортні системи та

системи будівництва. Ці рекомендації корисні для зацікавлених сторін, включаючи власників активів, постачальників продуктів і послуг.

Немає простого загального рішення, яке могло б задовольнити потреби безпеки для кожної системи. Організації мають різні потреби, а різні системи потребують різної сили механізмів захисту. Ту саму технологію можна застосовувати іншими способами та в різній мірі, залежно від потреб. SMM допомагає організаціям визначати пріоритети для покращення безпеки. Зрілість безпеки відображає належну відповідність вибору їхнім потребам.

Модель зрілості безпеки сприяє ефективній і продуктивній співпраці між діловими та технічними зацікавленими сторонами. Особи, які приймають бізнес-рішення, менеджери з бізнес-ризику та власники систем IoT, що реалізують стратегію впровадження практик безпеки з належною зрілістю, можуть співпрацювати з аналітиками, архітекторами, розробниками, системними інтеграторами та іншими зацікавленими сторонами, які відповідають за технічне впровадження. Вони також можуть враховувати точки зору регуляторів та інших сторін, наприклад, постачальників страхових послуг. Системні архітектори, дизайнери, тестувальники та інсталятори мають перевірити, чи правильно вибрано вимоги до програми, а реалізація правильно втілює ці вимоги.

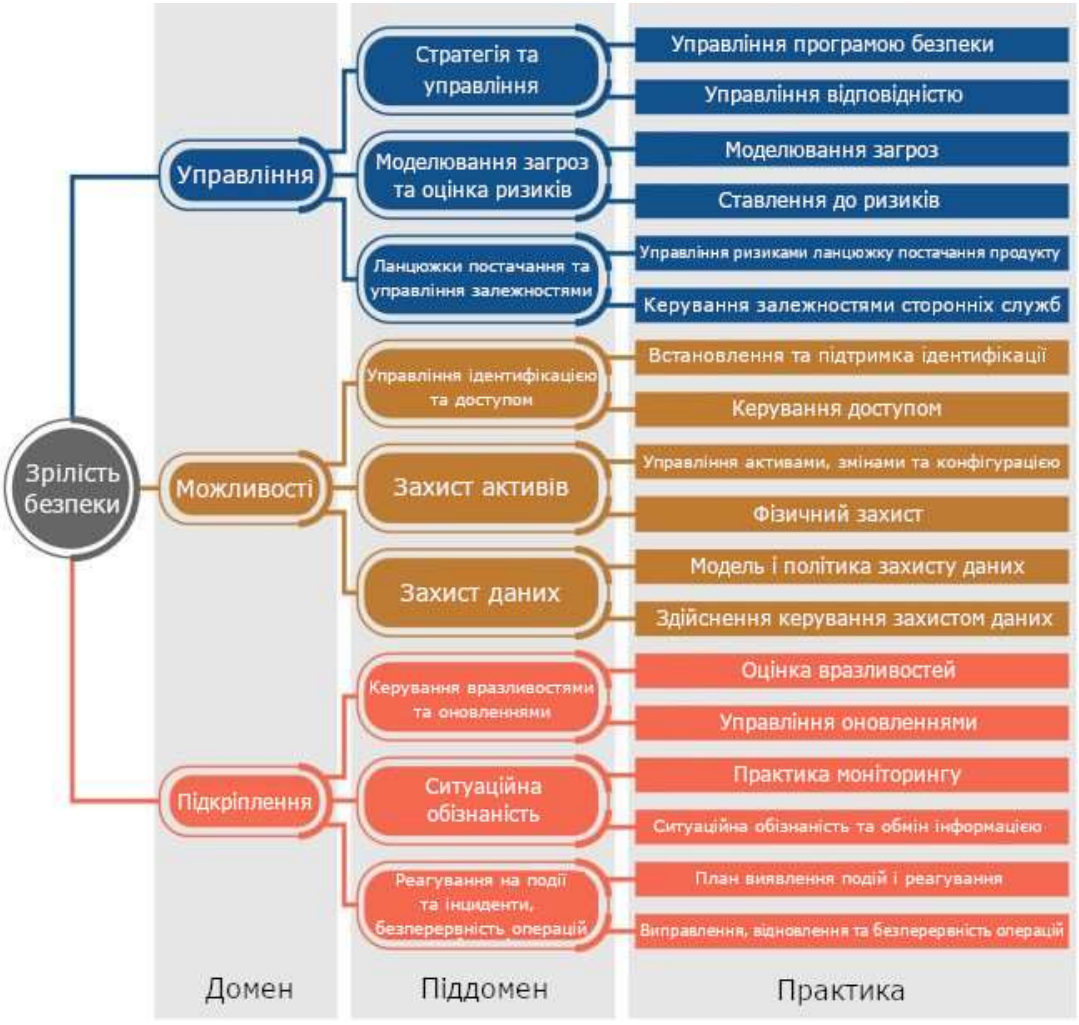

Рисунок 2 – Ієрархія складових моделі зрілості безпеки IoT

SMM визначає зрілість безпеки як ступінь впевненості в тому, що поточний стан безпеки відповідає всім потребам безпеки організації та всім вимогам, пов’язаним із безпе-

кою організації. Зрілість безпеки – це міра розуміння загального поточного підходу до безпеки, включаючи людей, процеси та технології, включаючи їх необхідність, переваги та вартість підтримки. Фактори, що сприяють цьому, включають конкретні загрози галузевій вертикалі організації, вимоги безпеки, нормативні, етичні вимоги та вимоги відповідності, профіль загрози організації та унікальні ризики, присутні в середовищі. Ієрархія складових моделі зрілості безпеки IoT представлена на рис. 2.

Існують два ортогональні виміри оцінки зрілості безпеки: комплексність і охоплення. Комплексність визначає ступінь глибини, узгодженості та надійності практик безпеки. Використання повноти в цій моделі зменшує складність, розглядаючи разом різні аспекти, такі як обізнаність про організаційну безпеку, ступінь впровадження практик і забезпечення практик (та їх еволюції). Наприклад, вищий рівень комплексності моделювання загроз передбачає більш автоматизований, систематичний і розширений підхід. Охоплення відображає ступінь відповідності потребам галузі або системи. Це фіксує ступінь налаштування заходів безпеки, які підтримують домени зрілості безпеки, піддомени або практики. Такі налаштування зазвичай потрібні для вирішення галузевих або системних обмежень систем IoT.

5. Висновки

Різноманітність, неоднорідність, складність і просторовий розподіл систем IoT спричиняють відповідні труднощі при побудові їхніх систем безпеки. Складність забезпечення безпеки Інтернету речей обумовлена обмеженнями пристроїв і відсутністю стандартів, у тому числі специфічних для Інтернету речей. IoT експоненціально стає частиною нашого повсякденного життя, щоб підвищити ефективність, надати необмежену кількість послуг, підвищити якість життя та забезпечити зручність за допомогою підключення різних технологій, пристроїв і програм. Оскільки кількість пристроїв Інтернету речей зростає та використовується в різних доменах і програмах, кількість загроз і величезних ризиків для безпеки та конфіденційності зростає, створюючи Інтернет вразливостей. Застосування знання-орієнтованого підходу дозволяє прискорити процес проєктування засобів безпеки для IoT з урахуванням специфіки сфери їх застосування на основі узагальненої онтології.

Проведений аналіз показує потребу в безпеці в контексті IoT і відмінність від інших систем через неоднорідність IoT. Представлено моделі безпеки IoT, які орієнтовані на вирішення питань безпеки та конфіденційності в IoT.

СПИСОК ДЖЕРЕЛ

1. The European Union Agency for Cybersecurity (ENISA). Baseline security recommendations for IoT. 2017. November 20. URL: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

2. ISO/IEC 20924:2021. Information technology – Internet of Things (IoT) – Vocabulary. 2021. URL: https://www.iso.org/standard/82771.html.

3. ITU-T, Y.2060: Overview of the internet of things, Technical report, International Telecommunication Union. 2012. URL: https://www.itu.int/rec/T-REC-Y.2060-201206-I.

4. Kovalenko O. Knowledge Driven Cyber-Convergent Systems Based on Situational Agents. *IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT)*. 2022. P. 243–246. DOI: 10.1109/CSIT56902.2022.10000762.

5. Kovalenko O. Systems Convergence for Situational Control and Decision Making in Distributed Environments. *IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. 2022. P. 344–347. DOI: 10.1109/TCSET55632.2022.9767006.

6. Ma J., Ning H., Huang R., Liu H., Yang L.T., Chen J., Min G. Cybermatics: A holistic field for systematic study of cyber-enabled new worlds. *IEEE Access*. 2015. Vol. 3. P. 2270–2280.

7. Madakam S., Ramaswamy R., Tripathi S. Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*. 2015. Vol. 3. P. 164–173. DOI: 10.4236/jcc.2015.35021.
8. Mullet V., Sondi P., Ramat E. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access*. 2021. Vol. 9. P. 23235–23263. DOI: 10.1109/ACCESS.2021.3056650.
9. Williams P., Dutta I.K., Daoud H., Bayoumi M. A survey on security in internet of things with a focus on the impact of emerging technologies. *Internet of Things*. 2022. Vol. 19. P. 100564. DOI: 10.1016/j.iot.2022.100564.
10. Ogunniye G., Kökciyan N. A Survey on Understanding and Representing Privacy Requirements in the Internet-of-Things. *Journal of Artificial Intelligence Research*. 2023. Vol. 76. P. 163–192. URL: https://jair.org/index.php/jair/article/view/14000.
11. Souag A., Mazo R., Salinesi C., Comyn-Wattiau I. Using the AMAN-DA method to generate security requirements: a case study in the maritime domain. Requirements Eng. 2018. Vol. 23, Issue 4. P. 557–580. DOI: 10.1007/s00766-017-0279-5.
12. Rueda-Rueda J.S., Jesus M.T., Portocarrero J.M.T. Framework-based security measures for Internet of Thing: A literature review. *Open Computer Science*. 2021. Vol. 11, N 1. P. 346–354. DOI: 10.1515/comp-2020-0220.
13. Kovalenko O., Kovalenko T. Knowledge Model and Ontology for Security Services. *2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC)*. Kyiv, Ukraine, 2018. P. 1–4. DOI: 10.1109/SAIC.2018.8516875.
14. Mozzaquatro B.A., Melo R., Agostinho C., Jardim-Goncalves R. An ontology-based security framework for decision-making in industrial systems. *2016 4th International Conf. on Model-Driven Engineering and Software Development (MODELSWARD)*. Rome, Italy, 2016. P. 779–788.
15. Souag A., Salinesi C., Mazo R., Comyn-Wattiau I. A Security Ontology for Security Requirements Elicitation / F. Piessens, J. Caballero, N. Bielova (eds.). *Engineering Secure Software and Systems (ESSoS 2015)*. Springer, Cham, 2015. Vol. 8978. P. 157–177. DOI: 10.1007/978-3-319-15618-7_13.
16. Zhang S., Bai G., Li H., Liu P., Zhang M., Li S. Multi-Source Knowledge Reasoning for Data-Driven IoT Security. *Sensor*s. 2021. Vol. 21. P. 7579. DOI: 10.3390/s21227579.
17. Damor D. IoT Security Threats and Solutions. URL: https://www.einfochips.com/blog/iot-security-threats-and-solutions/.
18. Banu N.M., Sujatha C. IoT Architecture a Comparative Study. *International Journal of Pure and Applied Mathematics*. 2017. Vol. 117, N 8. P. 45–49. DOI: 10.12732/ijpam.v117i8.10.
19. Cosman E., Gilsinn J., Hirsch F., Kobes P., Rudina E., Zahavi R. Industry IoT Consortium (IIC) and ISA. IoT Security Maturity Model: ISA/IEC 62443 Mappings for Asset Owners. Product Suppliers and System Integrators. 2023/08/09. URL: https://www.isagca.org/hubfs/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/SMM-62443-Asset-Owner-Product-Supplier-Service_20230809.pdf.

Стаття надійшла до редакції 05.09.2023