УДК 342.9:5.08 DOI: https://doi.org/10.32631/pb.2023.3.17

ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН,
Харківський національний університет внутрішніх справ,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0002-1020-9399,
e-mail: klimushyn@ukr.net;

ВІКТОРІЯ ЄВГЕНІВНА РОГ,
Харківський національний університет внутрішніх справ,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0002-7443-5125,
e-mail: vitochkarog@gmail.com;

ТЕТЯНА ПЕТРІВНА КОЛІСНИК,
Харківський національний університет внутрішніх справ,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0002-7442-8136,
e-mail: ktp201505@gmail.com

ПРАВОВІ АСПЕКТИ СТАНДАРТИЗАЦІЇ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Технології Інтернету речей надають розумним речам можливість прийняття рішень у системі управління фізичними об'єктами, використовуючи інтелект і консенсус. Для підтримки Інтернету речей задіяні такі технології, як вбудовані пристрої, хмарні і туманні обчислення, обробка великих даних, машинне навчання, штучний інтелект, що забезпечує виробництво інтелектуальних фізичних об'єктів. Огляд існуючих інфраструктур безпеки для інтелектуальних середовищ на основі Інтернету речей свідчить, що кожний підключений пристрій може стати потенційною точкою входу для атаки зловмисників.

Надано огляд ключових аспектів щодо стандартів безпеки розумних середовищ на основі Інтернету речей за напрямами: потенційних рішень, інтелектуальних середовищ, меж оцінки безпеки, відкритих проблем і викликів. Актуальним завданням є додаткові дослідження щодо розвитку методологічних і технологічних заходів стандартизації у сфері функціональної сумісності різнорідних пристроїв Інтернету речей із тим, щоб розпочати подальші дискусії щодо розробки нових стандартів безпеки та інфраструктури сертифікації розумних середовищ на основі Інтернету речей.

На основі аналізу існуючих проблем запровадження Інтернету речей досліджено методологічні і технологічні особливості правового регулювання інтелектуальних середовищ. Розглянуто структури стандартизації мереж і послуг середовищ Інтернету речей на регіональному, європейському та глобальному міжнародному рівнях.

Визначено архітектуру середовищ Інтернету речей – це багаторівнева, гетерогенна система зі складною топологією та використанням інноваційних технології. Визначено явище безпеки Інтернету речей як комплексне поняття, що включає в себе функціональну безпеку (*safety*) та інформаційну безпеку (*security*) з їх взаємозв'язком, протиріччями, викликами та ризиками.

Досліджено функціональна безпеку Інтернету речей у термінах функції безпеки, повноти безпеки та стійкості, які підлягають регламентації в технічних вимогах на виріб, що проєктується. Надано аспектну модель функціональної сумісності Інтернету речей і наведено приклади її застосування за взаємопов'язаними складовими (транспортна, синтаксична, семантична, поведінкова й аспект політики).

Проведено оцінку загальноприйнятих практик та ризиків створення регламентуючих документів (стандартів, інструкцій, методичних матеріалів) у сфері функціональної безпеки Інтернету речей. Надано рекомендації щодо запровадження науково обґрунтованого підходу до національної стандартизації безпеки Інтернету речей та заходів вирішення проблеми функціональної сумісності різнорідних пристроїв Інтернету речей.

Ключові слова: *Інтернет речей (IoT), стандарти безпеки, сертифікати безпеки, функціональна безпека, інформаційна безпека, функціональна сумісність.*

Оригінальна стаття

ВСТУП. Інтернет речей (*Internet of Things – IoT*) складається з двох ключових елементів: «інтернет» і «речі», що пов'язані один з одним через інтернет, і це дає їм змогу координувати свої дії і приймати рішення разом. Вони за допомогою технологій можуть чути, бачити, думати, обчислювати і діяти. Ці технології дають розумним речам змогу приймати рішення у системі управління фізичними об'єктами, використовуючи інтелект і консенсус. У результаті створюють виклики, які вимагають спеціалізованих стандартів безпеки Інтернету речей (Salman, Jain, 2017).

Отже, Інтернет речей (далі – IoT) є технологією доступу об'єктів фізичного світу до інтернету, яка забезпечує можливість ідентифікації різним об'єктам фізичного світу, наділяючи їх інтелектуальною поведінкою за допомогою забезпечення середовища для обміну інформацією один з одним та з хмарою в режимі реального часу без безпосередньої участі людини (Vermesan, Friess, 2014).

Технологія IoT здійснила революційний вплив у багатьох сферах нашого життя. Цей вплив став ключовим чинником інновацій та успіху в широкому діапазоні сфер, враховуючи розумні середовища на основі IoT (Karie, Sahri, Haskell-Dowland, 2020). Для підтримки IoT задіяні такі технології, як вбудовані пристрої, хмарні і туманні обчислення, обробка великих даних, машинне навчання, штучний інтелект, що забезпечують виробництво інтелектуальних фізичних об'єктів (Дявіл, Ноздріна, 2020).

Проте огляд існуючих інфраструктур безпеки для інтелектуальних середовищ на основі IoT свідчить, що кожний підключений пристрій може стати потенційною точкою входу для атаки зловмисників (Kebande, Karie, Venter, 2018).

Зіткнувшись із проблемами безпеки в середовищах на основі IoT, виникає потреба огляду існуючих традиційних стандартів безпеки та систем оцінювання, висвітлюючи їх основні сфери, щоб виявити ті, які потенційно можуть задовольнити деякі потреби безпеки на основі IoT. Результати цього дослідження можуть допомогти фахівцям-практикам, дослідникам та іншим зацікавленим особам зрозуміти сучасний стан сфери, а також допомогти їм визначити нові напрями досліджень і розпочати подальші дискусії щодо розробки нових стандартів безпеки та систем оцінки для вирішення існуючих і майбутніх проблем безпеки в розумних середовищах на основі IoT.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. *Метою* статті є визначення сутності й проблематики питання стандартизації і сертифікації функціональної безпеки інтелектуальних середовищ IoT на основі позитивного зарубіжного досвіду.

Для досягнення вказаної мети були поставлені такі *завдання*:

– визначити проблеми запровадження IoT для того, щоб виявити методологічні та технологічні основи правового регулювання інтелектуальних середовищ;

– розглянути структури стандартизації мереж і послуг середовищ IoT на регіональному європейському та глобальному міжнародному рівнях;

– встановити архітектуру середовищ IoT як багаторівневої, гетерогенної системи зі складною топологією та використанням інноваційних технології;

– розкрити комплексне поняття безпеки IoT як єдине явище з двома сторонами функціональної та інформаційної безпеки;

– дослідити функціональну безпеку IoT у термінах «функція безпеки» та «повнота безпеки», які підлягають регламентації в технічних вимогах на виріб, що проєктується;

– визначити аспектну модель функціональної сумісності IoT і навести приклади її застосування за взаємопов'язаними складниками;

– оцінити загальноприйняті практики та їхні ризики створення регламентуючих документів (стандартів, інструкцій, методичних матеріалів) у сфері функціональної безпеки IoT;

– проаналізувати чинне законодавство України у сфері IoT і штучного інтелекту та надати рекомендації щодо запровадження науково обґрунтованого підходу до стандартизації безпеки IoT;

– запропонувати заходи щодо вирішення проблеми функціональної сумісності різнорідних пристроїв IoT.

ОГЛЯД ЛІТЕРАТУРИ. Основоположним документом із функціональної безпеки є міжнародний стандарт IEC 61508-1 «Функціональна безпека електричних / електронних / програмованих електронних систем безпеки»[1], прийнятий Міжнародною електротехнічною комісією (*International Electrotechnical Commission – IEC*). Цей стандарт визначає функціональну

[1] Functional safety of electrical/electronic/ programmable electronic safety-related systems. Part 1: General requirements. IEC 61508-1. Edition 2.0. Geneva : International Electrotechnical Commission, 2010. URL: https://webstore.iec.ch/preview/info_iec61508-1%7Bed2.0%7Db.pdf (дата звернення: 15.04.2023).

безпеку як частину загальної безпеки, яка залежить від правильного функціонування систем і зовнішніх засобів зниження ризиків.

Стандарт визначає два фундаментальні принципи: забезпечення безпеки на основі передового досвіду протягом усього життєвого циклу і ймовірнісний характер відмов пристроїв на безпеку. Стандарт складається із семи частин, які згруповані за напрямами: визначення, нормативні вимоги стандарту та інформативні вказівки для розробки. У стандарті визначено методи забезпечення функціональної безпеки для кожної фази життєвого циклу електронних систем.

На основі IEC 61508-1 написано багато статей і монографій, у яких досліджені проблеми використання стандарту за сферами впровадження електронних систем.

Так, у роботі В. О. Остапенка (2017) розкрито методи оцінки функціональної безпеки бездротової сенсорної мережі моніторингу стану рослин з вираховуванням двох типів відмов: систематичних і випадкових.

У роботі Д. Ю. Хлапоніна (2018) проаналізовано законодавство та результати наукових досліджень у сфері кіберфізичних систем за вимогами надійності, безпеки, стійкості та конфіденційності таких країн, як Велика Британія, Німеччина, США, а також у Європейському Союзі. У дослідженні визначено, що численні зусилля різних міжнародних організацій у сфері створення стандартів кіберфізичних систем виявилися недостатніми і досі не забезпечили повної їх сумісності.

Аналіз останніх наукових досліджень, проведених у галузі вирішення питань інформаційної безпеки і конфіденційності даних IoT, показав, що вони ґрунтуються на традиційних методах безпеки мережі. Тому актуальним є питання розробки механізмів безпеки IoT-пристроїв як гетерогенних багаторівневих систем.

У дослідженні Н. М. Карі, Н. М. Сахрі та П. Хаскелл-Доуленда (2020) надано огляд ключових аспектів щодо стандартів безпеки розумних середовищ на основі IoT за напрямами: потенційних рішень, інтелектуальних середовищ, рамок оцінки безпеки, відкритих проблем та викликів. Як новий внесок у цьому документі запропоновано таксономію, яка класифікує різні виклики та потенційні рішення виявлених проблем у середовищі IoT.

Багато науковців розглядають актуальне завдання вітчизняного законодавства щодо стандартизації розробки та впровадження штучного інтелекту за різними сферами застосування (Іванов, Бершадська, 2022; Токарєва, Савліва, 2021; Тюря, 2022). Вітчизняне законодавство з регламентації використання інтелектуальних середовищ має бути комплексним, враховувати відомі міжнародні стандарти та рекомендації. Насамперед потрібно уніфікувати термінологію, узагальнити національні теоретичні напрацювання та практики, визначити проблеми забезпечення функціональної сумісності й безпеки розумних систем IoT.

Отже, актуальним завданням є додаткові дослідження щодо розвитку методологічних і технологічних заходів стандартизації у сфері функціональної сумісності різнорідних пристроїв IoT для того, щоб розпочати подальші дискусії стосовно розробки нових стандартів безпеки та інфраструктури сертифікації розумних середовищ на основі IoT.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. Методологія дослідження базується на аналізі зарубіжного досвіду впровадження технологій IoT. У процесі аналізу ми спиралися на відомі міжнародні документи, які регламентують сферу стандартизації безпеки IoT, результати наукових досліджень, опубліковані у відкритих виданнях.

Під час проведення дослідження були використані систематичні методи теоретичного обґрунтування проблеми. Згадані методи вказують на необхідність визначення ключової сфери дослідження, вибірки, вилучення корисних даних та інтерпретації їх достовірності. Наше дослідження передусім було зосереджене на визначенні відповідних статей щодо стандартів безпеки, зокрема спеціальних стандартів безпеки IoT, які перевіряють їх, щоб визначити, чи відповідають вони запропонованому системному критерію відбору.

Методологія огляду, використана в цьому дослідженні, має три основні етапи:

1) ідентифікація сфери дослідження, визначення питань дослідження, вибірка та визначення ключової стратегії або критеріїв пошуку. Ідентифікація досліджуваної сфери в контексті цієї статті ґрунтувалася на кількох дослідницьких питаннях аналізу поточного стану традиційних стандартів безпеки щодо проблем безпеки інтелектуальних середовищ на основі IoT, розгляді релевантних недоліків загальних стандартів безпеки та спеціальних стандартів безпеки IoT;

2) застосування стратегії або критеріїв пошуку до відомої літератури, проведення загального пошуку, пошуку в базі даних, оцінка пошуку та визначення критеріїв відбору;

3) узагальнення відібраної літератури, статей, існуючих стандартів, інструкцій та

методичних рекомендацій для вирішення проблеми функціональної сумісності та безпеки різнорідних пристроїв IoT.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. Головною тенденцією, характерною для IoT, так само, як і його головною проблемою, є досить швидке збільшення кількості кінцевих пристроїв, підключених до мережі. Зі зростанням кількості розумних пристроїв виникають і недоліки, пов'язані з керуванням великим потоком даних, створюваних цими пристроями, а також з вибором найбільш вдалого рішення під час розгортання мереж із таких пристроїв та забезпеченням взаємодії всередині мережі.

Значна конкуренція між виробниками у сфері IoT робить взаємодію між інтелектуальними пристроями ще складнішим завданням. Відсутність єдиного стандарту та напрацьованих практик безперешкодної і стійкої взаємодії різних пристроїв зараз є однією з основних проблем. Варто враховувати, що наявність цієї проблеми значно впливає на безпеку всередині мереж IoT.

Поточну ситуацію слід охарактеризувати як конкуренцію стандартів. Можна виокремити кілька консорціумів та спілок, які були створені для формування та розвитку стандартів взаємодії, зв'язку, конфіденційності та безпеки.

Існують різні світові організації, що займаються питаннями стандартизації: Інститут інженерів з електротехніки та електроніки (*Institute of Electrical and Electronics Engineers – IEEE*), Національний інститут стандартів і технологій (*National Institute of Standards and Technology – NIST*), Європейський інститут стандартів телекомунікацій (*European Telecommunications Standards Institute – ETSI*), Міжнародна організація для стандартизації (*International Organisation Standardisation – ISO*).

Питаннями стандартизації мереж і послуг IoT на регіональному європейському рівні займається Європейський інститут стандартів телекомунікацій, у якому створено спеціальний технічний комітет «Розумний міжмашинний зв'язок» (*Smart Machine-to-Machine Communications – SmartM2M*).

На глобальному рівні основними організаціями, залученими до стандартизації IoT, є:

– сектор стандартизації Міжнародного союзу електрозв'язку (*International Telecommunication Union – ITU*), в межах якого є дослідницька комісія – ДК20 «IoT і його додатки, враховуючи "розумні" міста та спільноти»;

– партнерський проєкт oneM2M, що реалізує ініціативу глобального партнерства між вісьмома провідними світовими організаціями з розробки стандартів: ARIB (Японія), ATIS (США), CCSA (Китай), ETSI (Європа), TIA (США), TSDSI (Індія), TTA (Корея) і TTC (Японія) разом із галузевими форумами та консорціумами для розробки специфікацій, які забезпечують найефективніше розгортання міжмашинних (M2M) систем зв'язку та IoT (Домрачева, Довженко, Дмитренко, 2019).

Зусилля світової телекомунікаційної спільноти спрямовані на розвиток нових сегментів ІКТ-ринку, пов'язаних з IoT. Нормативно-технологічною базою цього розвитку в умовах подальшої лібералізації ринків стають відкриті стандарти, що створюються на глобальному та регіональному рівнях.

Участь у роботі міжнародних організацій зі стандартизації IoT з боку українських наукових організацій на сьогодні незначна через відсутність фінансування міжнародних програм, що призводить до технологічного відставання у використанні IoT, втрати компетенцій та міжнародного статусу України як технологічного партнера.

Архітектура IoT – це структура та організація компонентів, що утворюють мережу IoT. Вона визначає спосіб, яким пристрої IoT підключаються до мережі, взаємодіють та обмінюються даними. Залежно від сфери застосування можуть використовуватися різні архітектури мереж IoT, які відрізняються своїми характеристиками та продуктивністю. Найбільш поширена архітектура має чотири рівні (Sethi, Sarangi, 2017; Chintham, Poladi, Kumar, 2018) (див. рис. 1):

1) *сенсорний рівень* – є ключовим рівнем, що має датчики, пристрої, виконавчі механізми тощо, які збирають дані з фізичного середовища, обробляють їх і потім надсилають через мережу;

2) *мережевий рівень* – складається з мережевих шлюзів і систем збору даних, який перетворює аналогові дані у цифрові. Для утворення цього рівня архітектури використовують такі протоколи і технології (Пулеко, Єфіменко, 2022), як Wi-Fi, Bluetooth, ZigBee, Z-Wave, 6LoWPAN, LoRaWAN, NB-IoT, Ethernet тощо;

3) *рівень обробки даних* – реалізує попередню обробку даних за різновидом і використовує такі технології: візуалізаційні інструменти, Big Data, методи та алгоритми штучного інтелекту;

4) *рівень додатків* – складається з хмарних центрів, туманних технологій, де дані керуються та використовуються програмами в різних сферах (Пулеко, Єфіменко, 2022): системи

автоматизації будівель та офісів, розумні системи відслідковування даних про здоров'я людини, системи моніторингу роботизованих виробничих ліній, системи автоматизації логістики та транспорту, системи управління громадською безпекою.

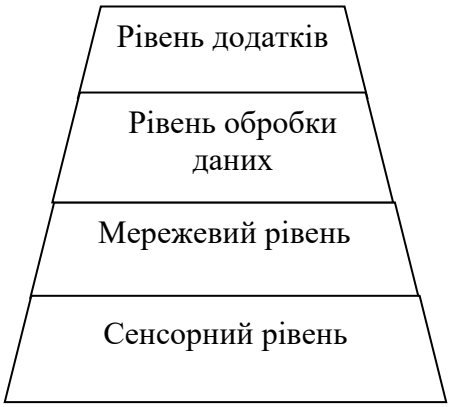

Рис. 1. Багаторівнева архітектура IoT

IoT сприяє вирішенню завдань людства в таких сферах, як громадська безпека, управління процесами, сервіс життя людей, медичні послуги, продуктивність і конкурентоспроможність бізнесу. Однак розумні речі не лише покращують якість життя, а й стають джерелом загроз конфіденційності та громадській безпеці.

Одна з найважливіших особливостей IoT – можливість безпосередньо взаємодіяти з навколишнім середовищем та впливати на нього. IoT є гетерогенною системою зі складною топологією, що поєднує в собі різні старі та нові технології. Умови та ситуації, в яких функціонують IoT, значно різняться, причому не лише залежно від належності до одного із сегментів, а й секторів. Навіть всередині одного сегмента цілі використання тих самих речей можуть бути різними, що виявляється у різниці вимог до безпеки пристроїв та систем.

Дуже важливою відмінністю є те, що безпека IoT стає комплексним поняттям, яке містить у собі не лише традиційну інформаційну безпеку (*security*), а й функціональну безпеку (*safety*), що відповідає за надійне функціонування цілої системи та окремих складників її пристроїв. Якщо інформаційна безпека стала критичною з появою інтернету, то функціональна безпека розглядалася і до появи цифрового управління, адже аварії відбувалися завжди, тобто захисту потребує і сам фізичний пристрій IoT. Тож інформаційна та функціональна безпека є сторонами того самого явища. При цьому між функціональною та інформаційною безпекою можуть виникати серйозні суперечності (Cerf et al., 2016).

Необхідно враховувати функціональну безпеку в системі IoT, оскільки пристрій може працювати безпечно за нормального використання, але якщо пристрій вийшов з ладу, зловмисник спробує маніпулювати функціями пристрою, завдаючи шкоди об'єктам, що контролюються пристроєм, або порушити конфіденційність людей, які пов'язані з ним (Atlam, Wills, 2020).

Існують серйозні проблеми стосовно безпеки через відкриті та невикористані порти пристроїв IoT, оскільки це дає змогу зловмисникам впроваджувати шкідливі коди, завдаючи шкоди пристроям, особливо критичним для безпеки. Таким чином, це питання має бути розглянуте в майбутньому проєктуванні пристроїв для підтримання фізичної та інформаційної безпеки пристроїв IoT.

Передбачається, що в майбутньому завдяки об'єднанню кіберпростору із фізичним простором буде реалізовано широкий спектр нових механізмів і послуг. Використання цих механізмів дасть змогу розробникам послуг класифікувати, проаналізувати та зменшити приховані ризики пристроїв і систем, що об'єднають фізичний і кіберпростір, кількісно оцінити перспективи бажаних вимог до функціональної та інформаційної безпеки і порівняти їх. Завдяки цьому, навіть якщо перевірки проводитимуться за допомогою окремих процесів, можна забезпечити узгодженість перспектив і змісту заходів у цих просторах, необхідних у відповідних пристроях і системах (Saracco, 2019).

Проте необхідно враховувати, що ефект і розмір впливу відрізняються залежно від призначення пристроїв і систем IoT. Це буде основою для належного аналізу впливу у випадку, якщо стався інцидент, з точки зору користувача механізмів і послуг, класифікуючи їх відповідно до вимог загальної безпеки.

Таким чином, у майбутньому необхідно створити ґрунтовні умови для продовження розробки системної відповіді на належне впровадження заходів функціональної та інформаційної безпеки, де широко використовується IoT, а кіберпростір і фізичний простір є високо інтегрованими структурами суспільства (Ning, Zhang, Daneshmand, 2021).

Інформаційна безпека IoT – це дія, спрямована на забезпечення безпеки пристроїв та мереж, до яких вони підключені, від загроз і витоку даних за допомогою захисту, ідентифікації та відстеження ризиків, а також усунення вразливостей на різних пристроях. Властивість інформаційної безпеки має забезпечити доступність, цілісність і конфіденційність даних системи управління.

Вимоги безпеки IoT можуть бути реалізовані лише за допомогою комплексних рішень, що забезпечують видимість, сегментацію та захист усієї мережної інфраструктури. Ці рішення повинні мати такі ключові можливості:

– *упізнати* – ідентифікувати та класифікувати IoT-пристрої для побудови профілю ризику;

– *розділити* – розуміти області атаки IoT із поділом на групи на базових правилах, зважаючи на їхні профілі ризику;

– *захистити* – застосувати політики безпеки на різних рівнях інфраструктури (Pal et al., 2020).

У свою чергу завданням кібербезпеки є захист від атак, спрямованих на обмеження готовності, цілісності та конфіденційності даних. Завдання реалізується за допомогою профілактичних або активних технічних та організаційних заходів. Недооцінка аспектів інформаційної безпеки під час організації функціональної безпеки може мати прямі наслідки для виробничого устаткування. Також можливий непрямий вплив на виробничий процес, а отже, і на кінцевий продукт.

Функціональна безпека IoT безпосередньо пов'язана з надійністю апаратного та програмного складника, на яких покладаються управління функціями безпеки. Фізичні об'єкти, якими управляють пристрої IoT, найчастіше створюють ризики для довкілля та людей. Ці системи управління повинні виконувати функції безпеки і мати певні характеристики (резервування, стійкість до відмов, самодіагностика, стійкість до зовнішніх екстремальних впливів тощо). Контроль за розробкою, впровадженням та експлуатацією комп'ютерних систем управління, важливих для безпеки, здійснюється державними органами сертифікації та ліцензування. Тобто проєктування систем IoT має проводитися з дотриманням вимог до функціональної безпеки.

Для кращого розуміння проблеми функціональної безпеки наведемо деякі терміни, що стосуються функцій безпеки та повноти безпеки, які підлягають регламентації в технічних вимогах на виріб, що проєктується.

1. *Функція безпеки (safety function)* – функція, що реалізується системою та призначена для досягнення або підтримання безпечного стану обладнання стосовно конкретної небезпечної події.

2. *Повнота безпеки (safety integrity)* – ймовірність того, що система задовільно виконуватиме необхідні функції безпеки за всіх зазначених умов протягом заданого інтервалу часу.

3. *Повнота безпеки програмного забезпечення (software safety integrity)* – складник повноти безпеки системи, що стосується систематичних відмов, які виявляються в небезпечному режимі та стосуються програмного забезпечення.

4. *Повнота безпеки, що стосується систематичних відмов (systematic safety integrity)* – складник повноти безпеки системи, що стосується систематичних відмов, які виявляються у небезпечному режимі.

5. *Повнота безпеки апаратних засобів (hardware safety integrity)* – це складник повноти безпеки системи, що стосується випадкових відмов апаратури, які виявляються у небезпечному режимі.

6. *Рівень повноти безпеки (safety integrity level)* – дискретний рівень (приймає одне з чотирьох можливих значень), що відповідає діапазону значень повноти безпеки. При цьому рівень повноти безпеки, що дорівнює чотирьом, є найвищим рівнем повноти безпеки, а рівень повноти безпеки, що дорівнює одиниці, відповідає найменшій повноті безпеки.

7. *Стійкість до систематичних відмов (systematic capability)* – міра впевненості (виражена у чотирирівневому діапазоні) в тому, що систематична повнота безпеки елемента відповідає вимогам заданого значення рівня повноти безпеки певної функції безпеки елемента.

Зазначимо, що наведені вище терміни належать до систем, пов'язаних із безпекою, тобто до систем, які реалізують необхідні функції безпеки для досягнення та підтримання безпечного стану обладнання.

Стандарт функціональної сумісності систем IoT забезпечують проєктування систем IoT таким чином, щоб сутності системи IoT могли здійснювати обмін та спільне використання інформації. У системах IoT, де можуть бути підключені різні об'єкти, виникають складнощі від технологічних аспектів до глобальної політики, регулювання і міжнародного права.

Стандарт функціональної сумісності визначає різні характеристики з погляду аспектів, де кожен аспект характеризує один параметр. Для досягнення функціональної сумісності важливо, щоб усі аспекти були вивчені та спільно узгоджені взаємодіючими сутностями.

Аспектна модель функціональної сумісності має п'ять аспектів, які показані на рис. 2. Ця модель спочатку була розроблена у стандарті[1]

[1] ISO/IEC 19941:2017. Information technology – Cloud computing – Interoperability and portability // ISO : сайт. URL: https://www.iso.org/standard/66639.html (дата звернення: 15.04.2023).

і отримана шляхом об'єднання та абстрагування з європейською структурою сумісності[1].

Рис. 2. Аспекти функціональної сумісності IoT

Транспортна функціональна сумісність – це спільність інфраструктури зв'язку обмінюватись даними між сутностями. Вона містить у собі фізичний рівень (наприклад, дротовий або бездротовий зв'язок) і механізм передачі між різними сутностями системи IoT або між різними системами IoT. Цей механізм визначений як модельний на основі сутностей стандартизованої еталонної архітектури IoT із використанням загального словника, проєктів для багаторазового використання та найкращих галузевих практик[2].

Приклади транспортної функціональної сумісності:

1) IEEE 802.3 – це робоча група стандартних специфікацій[3] для Ethernet – методу фізичного зв'язку на основі пакетів у локальній мережі. Фізичний зв'язок здійснюється між вузлами або пристроями, такими як маршрутизатори, комутатори та концентратори, за допомогою мідних або оптоволоконних кабелів. Загалом стандарти IEEE 802.3 визначають фізичні носії та робочі характеристики Ethernet. Сьогодні існує багато варіацій цього стандарту;

2) IEEE 802.11 – набір стандартів зв'язку[4] для комунікації в бездротовій локальній мережній зоні. Продукти стандарту тестуються на сумісність і сертифікуються організацією Wireless Ethernet Compatibility Alliance (WECA), яка зараз відома як Wi-Fi Alliance. Сумісні бездротові продукти, що пройшли випробування за програмою «Альянсу Wi-Fi», можуть бути марковані знаком Wi-Fi. Цей стандарт є найбільш прийнятним за побудови бездротових мереж;

3) MQTT (*Message Queuing Telemetry Transport*) – це клієнт-серверний стандартизований протокол[5] обміну повідомленнями, який досить спрощений, щоб його могли підтримувати наймініатюрніші пристрої з мінімальним обсягом доступних ресурсів, але при цьому він досить надійний, щоб гарантувати, що важливі повідомлення завжди дійдуть до місця призначення. Протокол MQTT працює поверх

[1] New European Interoperability Framework. Promoting seamless services and data flows for European public administrations. 2017 // European Union : сайт. URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf (дата звернення: 15.04.2023).

[2] ISO/IEC 30141:2018. Internet of Things (IoT) – Reference Architecture // ISO : сайт. URL: https://www.iso.org/standard/65695.html (дата звернення: 15.04.2023).

[3] IEEE 802.3 Ethernet Working Group. URL: https://www.ieee802.org/3/ (дата звернення: 15.04.2023).

[4] EEE 802.11™ Wireless Local Area Networks. URL: https://www.ieee802.org/11/ (дата звернення: 15.04.2023).

[5] ISO/IEC 20922:2016. Information technology – Message Queuing Telemetry Transport (MQTT) v3.1.1 // ISO : сайт. URL: https://www.iso.org/standard/69466.html (дата звернення: 15.04.2023).

протоколу TCP, але може також використовувати інші мережеві протоколи, що забезпечують упорядковані двоспрямовані з'єднання без втрат;

4) AMQP (*Advanced Message Queuing Protocol*) – це відкритий стандартизований протокол[1] прикладного рівня, призначений для забезпечення взаємодії між широким спектром різних додатків та систем, незалежно від їх внутрішнього пристрою. Протокол AMQP дозволяє різним платформам, які реалізовані різними мовами, обмінюватися повідомленнями, що може бути особливо корисно у гетерогенних системах.

Синтаксична функціональна сумісність – це здатність двох або більше систем чи пристроїв проводити обмін інформацією на основі синтаксисів, таких як формати, правила тощо.

Приклади синтаксисів для інформації включають OWL (*Web Ontology Language* – мова вебонтологій), RDFS (*Resource Description Framework Schema* – мова опису словників термінів), UML (*Unified Modelling Language* – уніфікована мова моделювання), XML (*eXtensible Markup Language* – розширювана мова розмітки), JSON (*JavaScript Object Notation* – текстовий формат даних).

Семантична функціональна сумісність – це здатність сутностей, що здійснюють обмін інформацією, розуміти значення моделі даних у контексті предметної галузі. Концепції предметної галузі у системі IoT варіюються і залежать від властивостей відповідних сутностей.

Семантична функціональна сумісність ґрунтується на моделях даних інформації, що передаються. Моделі даних залежать від властивостей задіяних сутностей і функціональних можливостей інтерфейсів з-поміж них.

Поведінкова функціональна сумісність сутності IoT визначається в описі інтерфейсу. Опис інтерфейсу включає в себе декларацію інтерфейсу, який надає служба, часто у вигляді інтерфейсу прикладного програмування (*Application Programming Interface – API*). Декларація інтерфейсу прикладного програмування визначає інтерфейс у вигляді набору операцій, що надаються, а також вхідних і вихідних даних для кожної операції. Стосовно опису інтерфейсу прикладного програмування функціональна сумісність поведінки вимагає надання додаткової інформації за очікуваними результатами кожної операції, враховуючи такі елементи, як попередні умови, постумови і будь-які послідовності операцій, які необхідні для успішного використання інтерфейсу. Аспект поведінкової функціональної сумісності абстрагується від деталей реалізації та описує поведінку сутностей IoT незалежно від уявлення.

Функціональна сумісність поведінки досягається, коли результати використання інформації обміну відповідають очікуваному результату. Сутність IoT спроєктована для певної мети або завдання. Однак фактичне використання сутності іншою сутністю може мати мету, відмінну від вихідної, без порушення інших аспектів сумісності.

Функціональна сумісність поведінки є особливо важливою, коли з'являється нова версія певної сутності (наприклад, виконавчого пристрою) з аналогічним інтерфейсом. У цьому випадку, хоча семантичні та синтаксичні елементи інтерфейсу можуть збігатися, поведінка може відрізнятися, що призведе до непередбачуваних результатів.

Функціональна сумісність політики визначається як здатність двох або більше систем взаємодіяти в межах правових та організаційних норм і принципів політики, що застосовуються до систем, що беруть участь. Цей аспект включає в себе урядові закони та норми, а також положення й умови політики, що застосовуються до користувача IoT або постачальника системи IoT, і організаційну політику взаємодії.

Одним із важливих чинників функціональної сумісності IoT є однакове розуміння семантичних та поведінкових аспектів, які відображають концепції в галузі інтересів.

Проблеми, пов'язані із семантикою даних, передбачуваним використанням та організаційними сутностями людей і процесів, а також з обмеженнями правової чи нормативної бази, як правило, вирішувати набагато складніше. Наприклад, транспортна функціональна сумісність забезпечить передачу даних з однієї системи до іншої, але політичні чи нормативні обмеження зроблять дані практично недоступними. Відсутність угоди про структури управління може створювати юридичні ризики, що перешкоджають обміну даними[2].

Повна функціональна сумісність двох систем потребує функціональної сумісності для

[1] ISO/IEC 19464:2014. Information technology – Advanced Message Queuing Protocol (AMQP) v1.0 specification // ISO : сайт. URL: https://www.iso.org/standard/64955.html (дата звернення: 15.04.2023).

[2] ISO/IEC 19941:2017. Information technology – Cloud computing – Interoperability and portability // ISO : сайт. URL: https://www.iso.org/standard/66639.html (дата звернення: 15.04.2023).

всіх аспектів взаємодії. Однак дві системи можуть успішно взаємодіяти, навіть якщо функціональну сумісність досягнуто не для всіх аспектів.

Традиційний підхід до вирішення проблем безпеки полягає в реалізації стандартів. За останні кілька років люди намагалися вирішувати проблеми безпеки IoT, застосовуючи безліч методик, правил та інших документів. Хоча стандарти призначені для консолідації галузей навколо загальноприйнятих передових практик, велика кількість регламентуючих документів створює роздроблену картину, викликаючи розбіжності з приводу того, що та як робити. Але можна отримати велику користь від розгляду різних стандартів та методик, навіть якщо визнаємо, що немає єдиної думки про найкращий спосіб захисту пристроїв IoT.

По-перше, розмежуємо документи, що стосуються внутрішнього пристрою, та документи, що визначають функціонал. Ці два аспекти взаємопов'язані, оскільки технічна оснащеність розширює можливості користувачів стосовно безпеки. І навпаки, те, що в конструкції пристрою не закладено, обмежує функціонал: наприклад, виключає безпечне оновлення програмного забезпечення, надійність наданих даних, ізоляцію та сегментацію в межах пристрою, своєчасні сповіщення про збої. Інструкції, надані виробниками, галузевими установами чи державними органами, можуть поєднувати обидва типи пояснювальних документів.

По-друге, розмежуємо методичні рекомендації та стандарти. Перші регламентують категорії завдань, другі – процеси та специфікації до виконання цих завдань. Те й інше важливо, але методичні матеріали більш актуальні та широко застосовуються, оскільки стандарти безпеки швидко застарівають і сфера їхньої дії часто обмежена. Водночас деякі стандарти надзвичайно корисні та визначають основні компоненти технології IoT. Поєднання методик і стандартів сприятиме ефективному управлінню технічною інфраструктурою.

У цій статті будемо посилатися на необхідність методик і стандартів, щоб надати розробникам та користувачам інструкції щодо усунення можливих проблем у роботі описуваних нами інструментів, технологій і процесів. Наведемо приклади стандартів, інструкцій та методичних матеріалів:

Стандарти. Технічна специфікація європейських стандартів ETSI з кібербезпеки IoT містить умови розробки безпечних пристроїв IoT. Національний інститут стандартів та технологій США (*National Institute of Standards and Technology – NIST*) та Міжнародна організація зі стандартизації (*International Organization for Standardization – ISO*) публікують низку стандартів, що підтримують захист пристроїв IoT.

Рекомендаційні матеріали. Національним інститутом стандартів та технологій США розроблено методичні рекомендації з безпеки у кіберпросторі пристроїв IoT, зокрема застосовні до володіння та експлуатації, рекомендації щодо безпеки та контролю безпеки IoT.

Інструкції та довідкові матеріали. Відкритий проєкт безпеки вебдодатків (*The Open Web Application Security Project – OWASP*) вийшов далеко за межі діяльності однойменної організації. Його список «Топ-10» стали потужною допомогою для розробників програмного забезпечення та використовуються для підвищення рівня безпеки у різних проєктах. Цей список має такий перелік ризиків розробки додатків IoT:

1) *слабкі, передбачувані або жорстко закодовані паролі.* Використання загальновідомих або незмінних облікових записів, що відкривають доступ до розгорнутих систем;

2) *небезпечні мережеві служби*. Непотрібні або небезпечні мережі на пристрої, особливо доступні ззовні, що загрожують конфіденційності або доступності інформації чи допускають віддалене управління;

3) *небезпечні інтерфейси інфраструктури*. Небезпечні вебінтерфейси, серверні API, хмарні та мобільні інтерфейси в інфраструктурі за межами пристрою. Відсутність автентифікації / авторизації та шифрування, а також відсутність фільтрації введення та виведення;

4) *блокування механізму безпечного оновлення*. Неможливість безпечно оновити пристрій. Сюди належить відсутність перевірки прошивки на пристрої, шифрування під час передачі, механізмів захисту відтоку даних та повідомлень про зміни безпеки через оновлення;

5) *використання небезпечних або застарілих компонентів*. Відкриває несанкціонований доступ сторонніх осіб до зашифрованих матеріалів. Враховує неправильне налаштовування середовища операційних систем. Використання незахищених програмних або апаратних компонентів сторонніх постачальників;

6) *недостатній захист персональних даних*. Персональна інформація користувача використовується небезпечно, неналежним чином або без дозволу;

7) *небезпечні передачі та зберігання даних*. Персональна інформація користувача, що зберігається на пристрої або в інфраструктурі,

використовується небезпечно або неналежним чином;

8) *відсутність менеджменту безпеки*. Відсутність контролю безпеки пристроїв, що перебувають у промисловій експлуатації, враховуючи моніторинг систем та засоби реагування на вторгнення;

9) *небезпечні налаштування за замовчуванням*. Пристрої або системи, що постачаються з небезпечними налаштуваннями за замовчуванням, у яких користувач не може змінювати конфігурацію;

10) *відсутність фізичного захисту*. Відсутність фізичного захисту, що заважає злочинцям отримати конфіденційну інформацію або локальний контроль над пристроєм.

Інші інструкції та довідкові матеріали мають: базовий план NIST щодо IoT, ресурси щодо оновлення та зміцнення безпеки Національного управління з телекомунікацій та інформації США (*National Telecommu nications and Information Administration – NTIA*) щодо IoT; базові рекомендації Європейського агентства з мережевої та інформаційної безпеки (*European Network and Information Security Agency – ENISA*) щодо захисту IoT; рекомендації та оцінку безпеки IoT Міжнародної асоціації глобальної системи мобільного зв'язку (*Global System for Mobile Communications' Association – GSMA*) та рекомендації фонду безпеки IoT (*IoT Security Foundation*).

У чинному законодавстві України немає чіткого розуміння специфіки IoT і штучного інтелекту, його правового статусу та правового регулювання. Частково це поняття закріплене в Законі України «Про захист персональних даних»[1]. У 2020 році уряд України схвалив Концепцію розвитку штучного інтелекту[2].

Серед першочергових проблем, які стоять на шляху до нормального функціонування в галузі штучного інтелекту, у Концепції визначено недосконалість насамперед правового регулювання штучного інтелекту, недосконалість законодавства про захист персональних даних і відсутність застосування таких технологій у судовій практиці. Із проєктів правового закріплення штучного інтелекту в Україні планують масштабну співпрацю з міжнародними організаціями та запровадження європейського досвіду, зокрема в розробці стандартів захисту прав і свобод учасників таких відносин та Етичного кодексу використання штучного інтелекту (Токарєва, Савліва, 2021).

Аналіз ситуації свідчить про необхідність використання комплексного та науково обґрунтованого підходу до забезпечення безпеки IoT. Це:

– *оцінка ризиків* – забезпечення конфіденційності, безпеки, запобігання шахрайським діям, кібератакам та крадіжкам інтелектуальної власності;

– *безпека на етапі проєктування* – орієнтована на безпеку в кінцевих вузлах через створення захищеного до злому апаратного та програмного забезпечення;

– *безпека даних* – упровадження криптографічних засобів автентифікації, шифрування й управління ключами для надійного зберігання на пристрої інформації та в процесі її передачі;

– *управління життєвим циклом* – забезпечення безпеки протягом усього життєвого циклу IoT.

Варто виокремити низку можливих заходів, які б певним чином вплинули на вирішення проблеми функціональної сумісності різнорідних пристроїв.

Необхідно виробити та використовувати мінімальні критерії для взаємодії (сумісності) пристроїв та програм різних виробників, зокрема з метою недопущення антиконкурентних практик, розвитку технологій і запобігання фрагментації.

Слід розглянути питання про обов'язок виробників надати будь-яким третім особам доступ до інтерфейсів прикладного програмування пристроїв та програм IoT, що може бути пов'язано з проблематикою недоторканності приватного життя користувачів і технологій.

Варіантом вирішення проблеми можуть стати спеціальні механізми передпродажної експертизи інтелектуальних пристроїв на їхню сумісність, ґрунтуючись на вироблених мінімальних вимогах щодо сумісності пристроїв IoT.

Ще одним заходом, який можна вжити, є розробка універсальної онтології, яка містила б усі необхідні знання, зокрема правила взаємодії між інтелектуальними пристроями, а також логіку роботи мереж IoT тощо.

ВИСНОВКИ. Використання парадигми IoT у різних сферах діяльності людини, а також активний її розвиток дають змогу говорити про

[1] Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 15.04.2023).

[2] Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р (дата звернення: 15.04.2023).

те, що за цією технологією майбутнє. Розумний будинок і розумне місто значно підвищили рівень комфортності та безпеки життя людей.

Однією з головних проблем є відсутність регламентуючих документів у галузі IoT, особливо між різними виробниками. Не існує офіційних правил безпеки, і виробники можуть не встановлювати механізми безпеки. Тому необхідно сприяти тому, аби вживати заходів безпеки. Останніми роками з'явилися сертифікати IoT. Водночас ЄС прийняв акт про кібербезпеку, щоб уніфікувати та регулювати сертифікацію безпеки в державах-членах. Відповідно до цього акта створено групу сертифікації кібербезпеки (*European Cybersecurity Certification Group – ECCG*).

Сьогодні існує комп'ютерна мережа реагування на надзвичайні ситуації (*Computer Emergency Response Team – CERT*) по всьому світу, яка забезпечує екстрену технологічну допомогу у фізичному та кіберпросторі з вирішення проблем із безпекою.

Водночас IoT вимагає стандартизованого підходу для IT-інфраструктури, схем ідентифікації, протоколів обміну даними та узгодження використовуваних частот. Проблема стандартизації поступово вирішується, але доки не буде розроблено єдиних правил та протоколів взаємодії інтелектуальних пристроїв, поки консорціуми не домовляться між собою та не укладуть відповідних угод, складнощі щодо безпеки мереж IoT не зникнуть. Однак науковою спільнотою та спільнотою розробників обговорюються заходи, які дозволять суттєво покращити ситуацію. Можливо, найближчим часом з'явиться рішення, яке влаштує всіх і буде застосовуватися повсюдно.

Правове регулювання стандартизації IoT потребує свого подальшого дослідження науковцями, насамперед стосовно визначення правових механізмів комплексної підтримки фізичної та інформаційної безпеки пристроїв IoT, що дасть змогу об'єднати фізичний простір із кіберпростором, кількісно оцінити перспективи бажаних вимог до функціональної та інформаційної безпеки та здійснити порівняння між пристроями IoT.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Домрачева К. О., Довженко Н. М., Дмитренко В. В. Аналіз технологій та стандартів зв'язку для мережі IoT. *Наукові записки Державного університету телекомунікацій*. 2019. № 3 (55). С. 54–62. DOI: https://doi.org/10.31673/2518-7678.2019.0305462.

2. Дявіл А. Г., Ноздріна Л. В. Інтернет речей як складова індустрії 4.0: проєктний підхід. *Вісник Університету банківської справи*. 2020. № 3 (39). С. 85–93.

3. Іванов А. Г., Бершадська Д. Р. Правове регулювання штучного інтелекту в ЄС: «європейський підхід» і виклики правам людини. *Юридичний науковий електронний журнал*. 2022. № 10. С. 697–699. DOI: https://doi.org/10.32782/2524-0374/2022-10/175.

4. Остапенко В. О. Методи оцінки функціональної безпеки бездротової сенсорної мережі моніторингу стану рослин. *Штучний інтелект*. 2017. № 3–4. С. 32–43.

5. Пулеко І. В., Єфіменко А. А. Архітектура та технології Інтернету речей : навч. посіб. Житомир : Держ. ун-т «Житомирська політехніка», 2022. 234 с.

6. Токарєва К. С., Савліва Н. О. Особливості правового регулювання штучного інтелекту в Україні. *Юридичний вісник*. 2021. Т. 3, № 60. С. 148–153. DOI: https://doi.org/10.18372/2307-9061.60.15967.

7. Тюря Ю. І. Деякі аспекти побудови нормативної бази адміністративно-правового регулювання діяльності зі створення, впровадження та використання штучного інтелекту в Україні. *Juris Europensis Scientia*. 2022. Вип. 5. С. 25–28. DOI: https://doi.org/10.32782/chern.v5.2022.5.

8. Хлапонін Д. Ю. Особливості нормативно-правового регулювання кіберфізичних систем у провідних країнах світу. *Право і суспільство*. 2018. № 2, ч. 2. С. 145–151.

9. Atlam H. F., Wills G. IoT Security, Privacy, Safety and Ethics // Digital Twin Technologies and Smart Cities / ed. by M. Farsi, A. Daneshkhah, A. Hosseinian-Far, H. Jahankhani. Switzerland : Springer Nature, 2020. DOI: https://doi.org/10.1007/978-3-030-18732-3_8.

10. Cerf V. G., Ryan P. S., Senges M., Whitt R. S. IoT safety and security as shared responsibility. *Business Informatics*. 2016. Vol. 1, No. 35. Pp. 7–19. DOI: https://doi.org/10.17323/1998-0663.2016.1.7.19.

11. Chintham S., Poladi P. K., Kumar S. N. Security Challenges and Issues of the IoT System. *Indian Journal of Public Health Research & Development.* 2018. Vol. 9, No. 11. Pp. 748–753. DOI: https://doi.org/10.5958/0976-5506.2018.01551.6.

12. Karie N. M., Sahri N. M., Haskell-Dowland P. IoT Threat Detection Advances, Challenges and Future Directions // Workshop on Emerging Technologies for Security in IoT (Sydney, Australia, 21 April 2020). Sydney, 2020. Pp. 22–29. DOI: https://doi.org/10.1109/ETSecIoT50046.2020.00009.

13. Karie N. M., Sahri N. M., Yang W., Valli C., Kebande V. R. A review of security standards and frameworks for IoT-based smart environments. *IEEE Access*. 2021. Vol. 9. Pp. 121975–121995. DOI: https://doi.org/10.1109/ACCESS.2021.3109886.

14. Kebande V. R., Karie N. M., Venter H. S. Adding digital forensic readiness as a security component to the IoT domain. *International Journal on Advancer Science Engineering and Information Technology.* 2018. Vol. 8. No. 1. DOI: https://doi.org/10.18517/ijaseit.8.1.2115.

15. Ning H., Zhang Z., Daneshmand M. PhiNet of Things: Things Connected by Physical Space From the Natural View. *IEEE Internet of Things Journal*. 2021. Vol. 8, Iss. 11. Pp. 8680–8692. DOI: https://doi.org/10.1109/JIOT.2020.3040441.

16. Pal S., Hitchens M., Rabehaja T., Mukhopadhyay S. Security Requirements for the Internet of Things: A Systematic Approach. *Sensors.* 2020. Vol. 20, No. 20. DOI: https://doi.org/10.3390/s20205897.

17. Salman T., Jain R. A Survey of Protocols and Standards for Internet of Things. *Advanced Computing and Communications*. 2017. Vol. 1, No. 1. https://arxiv.org/ftp/arxiv/papers/1903/1903.11549.pdf.

18. Saracco R. Digital Twins: Bridging Physical Space and Cyberspace. *Computer*. 2019. Vol. 52, Iss. 12. Pp. 58–64. DOI: https://doi.org/10.1109/MC.2019.2942803.

19. Sethi P., Sarangi S. R. Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering.* 2017. Vol. 1. DOI: https://doi.org/10.1155/2017/9324035.

20. Vermesan O., Friess P. Internet of Things – From Research and Innovation to Market Deployment. New York : River Publishers, 2014. 373 p.

Надійшла до редакції: 18.04.2023

Прийнята до опублікування: 25.05.2023

REFERENCES

1. Atlam, H. F., & Wills, G. (2020). IoT Security, Privacy, Safety and Ethics. In M. Farsi, A. Daneshkhah, A. Hosseinian-Far, & H. Jahankhani (Eds), *Digital Twin Technologies and Smart Cities*. https://doi.org/10.1007/978-3-030-18732-3_8.

2. Cerf, V. G., Ryan, P. S., Senges, M., & Whitt, R. S. (2016). IoT safety and security as shared responsibility. *Business Informatics, 1*(35), 7–19. https://doi.org/10.17323/1998-0663.2016.1.7.19.

3. Chintham, S., Poladi, P. K., & Kumar, S. N. (2018). Security Challenges and Issues of the IoT System. *Indian Journal of Public Health Research & Development, 9*(11), 748–753. https://doi.org/10.5958/0976-5506.2018.01551.6.

4. Diavil, A. H., & Nozdrina, L. V. (2020). The Internet of Things as a component of Industry 4.0: a project approach. *Bulletin of the University of Banking, 3*(39), 85–93.

5. Domracheva, K. O., Dovzhenko, N. M., and Dmytrenko, V. V. (2019). Analysis of technologies and connection standards for the IoT network. Scientific *Notes of the State University of Telecommunications, 3*(55), 54–62. https://doi.org/10.31673/2518-7678.2019.0305462.

6. Ivanov, A. H., & Bershadska, D. R. (2022). Legal regulation of artificial intelligence in the EU: The "European approach" and human rights challenges. *Juridical Scientific and Electronic Journal, 10*, 697–699. https://doi.org/10.32782/2524-0374/2022-10/175.

7. Karie, N. M., Sahri, N. M., & Haskell-Dowland, P. (2020, April 21). IoT *Threat Detection Advances, Challenges and Future Directions* [Conference presentation abstract]. Workshop on Emerging Technologies for Security in IoT. https://doi.org/10.1109/ETSecIoT50046.2020.00009.

8. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEE Access, 9*, 121975–121995. https://doi.org/10.1109/ACCESS.2021.3109886.

9. Kebande, V. R., Karie, N. M., & Venter, H. S. (2018). Adding digital forensic readiness as a security component to the IoT domain. *International Journal on Advancer Science Engineering and Information Technology, 8*(1). https://doi.org/10.18517/ijaseit.8.1.2115.

10. Khlaponin, D. Yu. (2018). Peculiarities of regulatory and legal regulation of cyber-physical systems in the leading countries of the world. *Law and Society, 2*(2), 145–151.

11. Ning, H., Zhang, Z., & Daneshmand, M. (2021). PhiNet of Things: Things Connected by Physical Space From the Natural View. *IEEE Internet of Things Journal, 8*(11), 8680–8692. https://doi.org/10.1109/JIOT.2020.3040441.

12. Ostapenko, V. O. (2017). Methods of assessment of functional safety wireless sensor network of plant condition. *Artificial Intelligence, 3–4*, 32–43.

13. Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). Security Requirements for the Internet of Things: A Systematic Approach. *Sensors, 20*(20). https://doi.org/10.3390/s20205897.

14. Puleko, I. V., & Yefimenko, A. A. (2022). *Architecture and technologies of the Internet of Things*. State University "Zhytomyr Polytechnic".

15. Salman, T., & Jain, R. (2017). A Survey of Protocols and Standards for Internet of Things. *Advanced Computing and Communications, 1*(1). https://arxiv.org/ftp/arxiv/papers/1903/1903.11549.pdf.

16. Saracco, R. (2019). Digital Twins: Bridging Physical Space and Cyberspace. *Computer, 52*(12), 58–64. https://doi.org/10.1109/MC.2019.2942803.

17. Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering, 1*. https://doi.org/10.1155/2017/9324035.

18. Tiuria, Yu. I. (2022). Some aspects of building a regulatory framework for the administrative and legal regulation of activities related to the creation, implementation and use of artificial intelligence in Ukraine. *Juris Europensis Scientia, 5*, 25–28. https://doi.org/10.32782/chern.v5.2022.5.

19. Tokarieva, K. S., & Savliva, N. O. (2021). Peculiarities of legal regulation of artificial intelligence in Ukraine. *Law Herald, 3*(60), 148–153. https://doi.org/10.18372/2307-9061.60.15967.

20. Vermesan, O., & Friess, P. (2014). *Internet of Things – From Research and Innovation to Market Deployment*. River Publishers.

Received the editorial office: 18 April 2023

Accepted for publication: 25 May 2023

PETRO SERHIIOVYCH KLYMUSHYN,
Kharkiv National University of Internal Affairs,
Department of Combating Cybercrime;
ORCID: https://orcid.org/0000-0002-1020-9399,
e-mail: klimushyn@ukr.net;

VICTORIIA YEVHENIVNA ROH,
Kharkiv National University of Internal Affairs,
Department of Combating Cybercrime;
ORCID: https://orcid.org/0000-0002-7443-5125,
e-mail: vitochkarog@gmail.com;

TETIANA PETRIVNA KOLISNYK,
Kharkiv National University of Internal Affairs,
Department of Combating Cybercrime;
ORCID: https://orcid.org/0000-0002-7442-8136,
e-mail: ktp201505@gmail.com

LEGAL ASPECTS OF FUNCTIONAL SECURITY STANDARDISATION OF THE INTERNET OF THINGS

IoT technologies provide smart things with the ability to make decisions in the management of physical objects using intelligence and consensus. To support the Internet of Things, technologies such as built-in devices, cloud and fog computing, big data processing, machine learning, and artificial intelligence are used to produce intelligent physical objects. A review of existing security infrastructures for IoT-based intelligent environments shows that every connected device can be a potential entry point for an attack.

An overview of the key aspects of security standards for smart environments based on the Internet of Things has been provided in the following areas: potential solutions, intelligent environments, limits of security assessment, open issues and challenges. Additional research on the development of methodological and technological standardisation measures in the field of interoperability of heterogeneous IoT devices is an urgent task in order to start further discussions on the development of new security standards and certification infrastructure for smart environments based on the IoT.

Based on the analysis of the existing problems of implementing the Internet of Things, the methodological and technological features of legal regulation of intellectual environments have been studied. The structures of standardisation of networks and services of the IoT environments at the regional, European and global international levels have been considered.

The architecture of the Internet of Things environments has been defined as a multi-level, heterogeneous system with a complex topology and the use of innovative technologies. The single phenomenon of IoT security has been identified as a complex concept that includes functional security and information security with their interconnection, contradictions, challenges and risks.

The functional security of the Internet of Things has been studied in terms of the security function, security completeness and resilience, which are subject to regulation in the technical requirements for the product being designed. An aspect model of IoT interoperability has been presented and examples of its application in terms of interrelated components (transport, syntactic, semantic, behavioural, and policy aspects) have been given.

An assessment of generally accepted practices and risks of creating regulatory documents (standards, instructions, methodological materials) in the field of functional security of the Internet of Things has been carried out. Recommendations for the introduction of a scientifically based approach to national standardisation of IoT security and measures to address the problem of interoperability of heterogeneous IoT devices have been provided.

Key words: *Internet of Things (IoT), security standards, security certificates, functional security, information security, interoperability.*

Цитування (ДСТУ 8302:2015): Клімушин П. С., Рог В. Є., Колісник Т. П. Правові аспекти стандартизації функціональної безпеки Інтернету речей. *Право і безпека*. 2023. № 3 (90). С. 200–213. DOI: https://doi.org/10.32631/pb.2023.3.17.

Citation (APA): Klimushyn, P. S., Roh, V. YE., & Kolisnyk, T. P. (2023). Legal aspects of functional security standardisation of the Internet of Things. *Law and Safety*, 3(90), 200–213. https://doi.org/10.32631/pb.2023.3.17.