УДК 004.056:683.281 DOI: https://doi.org/10.32631/pb.2025.2.05

ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН,
Харківський національний університет внутрішніх справ,
навчально-науковий інститут № 4,
кафедра протидії кіберзлочинності;
https://orcid.org/0000-0002-1020-9399,
e-mail: klimushyn@ukr.net

КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА СПЕЦІАЛІЗОВАНІ ПРОТОКОЛИ ЗВ'ЯЗКУ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Пристрої Інтернету речей характеризуються обмеженими ресурсами з погляду потужності, обробки даних, обсягу пам'яті та пропускної здатності. Через це традиційні протоколи, що стосуються мережевих операцій і безпеки, не можуть бути реалізовані у спеціальному середовищі Інтернету речей у їхньому поточному вигляді.
Для організації інформаційної взаємодії в мережі Інтернету речей необхідна стандартизація, оскільки без установленого регулювання, точних інструкцій і всесвітніх стандартів галузь зрештою зіткнеться із серйозними проблемами сумісності та безпеки. Крім того, багато пристроїв Інтернету речей обробляють конфіденційні дані, які мають здатність автономно збирати і поширювати на інші пристрої або в мережу. Наголошено на необхідності посилення заходів захисту даних і впровадження суворішого контролю для пристроїв Інтернету речей, що проходять автентифікацію та взаємодіють у мережі. Захист пристроїв Інтернету речей і протоколів зв'язку став першочерговою проблемою в нашому дедалі більш взаємозв'язаному світі.
Зазначено, що аналіз безпеки комунікаційних технологій Інтернету речей за спеціалізованими протоколами зв'язку через мережі з різною топологією, дальністю з'єднання та пропускною здатністю є актуальною проблемою, оскільки зростає кількість випадків порушення безпеки та конфіденційності в екосистемі Інтернету речей, яка постійно розширюється в різних секторах економіки та життя людства з упровадженням мільярдів різнорідних інтелектуальних пристроїв. Крім того, багато мереж Інтернету речей охоплюють широкий набір протоколів зв'язку, деякі з яких можуть не мати надійних функцій безпеки, що робить їх вразливими до атак.
Термін «комунікаційна технологія» використано для визначення протоколів зв'язку на кожному рівні архітектури платформи Інтернету речей. З метою покращення розуміння архітектури та використання технологій Інтернету речей у статті представлено таксономію, яка сприяє ефективному розподілу відповідних технологій Інтернету речей на протоколи канального рівня, протоколи мережевої інкапсуляції та протоколи маршрутизації відповідно до їхніх стандартів.
Проведене дослідження може спонукати науковців і практиків до розроблення нових і більш ефективних мережевих протоколів з урахуванням виявлених у статті поточних прогалин і недоліків.

Ключові слова: *Інтернет речей, архітектура Інтернету речей, безпека Інтернету речей, протоколи безпеки Інтернету речей, протоколи зв'язку Інтернету речей, мережеві протоколи, стільниковий зв'язок.*

Оглядова стаття

ВСТУП. Основними елементами Інтернету речей (*Internet of Things*, далі – IoT) є люди, речі, дані та процеси. Системи IoT спрямовані на об'єднання цих елементів у мережу, які взаємодіють між собою через дротове або бездротове середовище. Пристрої IoT класифікуються як датчики – збирають дані, приводи – впливають на дії, і шлюзи – як інтерфейси для зв'язку та автоматизації. У межах IoT дані надходять із датчиків, обробляються мікроконтролерами, зберігаються у хмарній базі даних, а їх аналіз здійснюється з використанням різних інструментів та мов програмування, таких як Python, C++, R, JavaScript тощо. Інтернет речей створено для посилення зв'язку між «людина – пристрій» (Human-to-Device, H2D; Device-to-Human, D2H), між пристроями (Device-to-Device, D2D) або між людьми (Human-to-Human, H2H).

Інтернет речей спричинив появу численних автономних застосунків у сфері охорони здоров'я, бізнес-рішень, «розумних» міст, домашньої та промислової автоматизації, інтелектуальних транспортних систем. Успіх IoT

полягає в розподіленому зборі, агрегації, обробці та аналітиці даних, що можуть виконуватися з будь-якого місця, зазвичай у форматі хмарної служби.

Як наслідок, для забезпечення сумісності всіх пристроїв IoT потрібні спеціалізовані протоколи зв'язку, стандартна структура, сумісність застосунків, розширені можливості обробки даних та інші компоненти (Клімушин, Рог, Колісник, 2023). Це реалізується таким чином (Gerodimos et al., 2022): «розумний» об'єкт передає дані, зібрані його датчиками (фізичним світом), до центру обробки даних (локального чи хмарного) або навіть до іншого «розумного» об'єкта через проміжне з'єднання – шлюз. Використання шлюзу не є обов'язковим, оскільки потенційно смарт-об'єкт також може виконувати функції шлюзу. Потім дані, отримані на іншому боці, обробляються і можуть ініціювати кілька дій. Саме ці дії ускладнюють реалізацію систем, оскільки потребують вищого рівня сумісності для ефективного керування чи моніторингу фізичного світу.

У роботі М. Алама, К. А. Шакіла та С. Хан (2020) розглянуто широкий спектр спеціалізованих протоколів для забезпечення безпечної взаємодії «розумних» об'єктів, що робить навколишнє середовище більш інтелектуальним і здатним до швидкого реагування, сприяючи злиттю цифрового та фізичного світів. Слід зауважити, що взаємозв'язок пристроїв IoT відкриває низку загроз безпеки для користувачів, які можуть бути підключені до критичних систем (Maglaras et al., 2019).

Кожен пристрій зазвичай підключається до інтернету за допомогою інтернет-протоколу (далі – IP), але також може бути підключений локально через Bluetooth, NFC (зв'язок ближнього поля) тощо. Деякі відмінності між цими типами підключень полягають у споживаній потужності, радіусі дії та навантаженні на процесор. IP-з'єднання є складними та вимагають збільшення потужності й пам'яті, проте не мають обмежень щодо діапазону дії. Натомість з'єднання Bluetooth є простішим і потребує менше енергії та пам'яті, але має обмежений радіус дії.

Окремі пристрої, як-от смартфони та персональні комп'ютери, використовують мережеві протоколи для зв'язку. Водночас загальні протоколи, що використовуються цими пристроями, можуть не відповідати певним вимогам, таким як пропускна здатність, затримка й енергоспоживання. З огляду на те, що енергоспоживання є ключовим чинником під час проєктування мереж IoT, перевага надається технологіям бездротових мереж із низьким енергоспоживанням.

Вибір оптимального протоколу IoT передбачає ретельне зважування таких критеріїв, як бажаний діапазон застосування, граничний рівень енергоспоживання, пропускна здатність, затримка, якість обслуговування – і все це розглядається крізь призму безпеки. Більшість протоколів безпеки для IoT розроблені з урахуванням роботи на кількох рівнях архітектури з метою забезпечення надійного захисту системи.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. *Метою* статті є порівняльний аналіз безпеки та продуктивності протокольних комунікаційних технологій пристроїв IoT в ієрархічній архітектурі їхньої взаємодії з урахуванням відмінностей за масштабом, ресурсами, пропускною здатністю, енергоспоживанням, розміром і затримкою повідомлень, сумісністю та надійністю.

Для досягнення зазначеної мети поставлено такі *завдання*:

– проаналізувати стандартну архітектуру IoT за трьома основними рівнями: рівень сприйняття, мережевий рівень і прикладний рівень;

– визначити протоколи обміну повідомленнями, аналізу стану та керування за рівнями взаємодії мереж IoT;

– охарактеризувати вимоги до безпеки IoT за п'ятьма категоріями: безпека мережі, управління ідентифікацією та доступом, конфіденційність, довіра та стійкість;

– здійснити порівняльний аналіз загроз і ризиків кібербезпеки IoT при використанні різних протоколів зв'язку;

– визначити особливості протоколів фізичного рівня, рівня керування доступом до середовища передавання даних IoT згідно зі стандартом IEEE 802.15.4;

– проаналізувати безпеку та продуктивність спеціалізованих протоколів зв'язку IoT (IEEE 802.15.4, NFC, Zigbee, BLE, RPL, 6L0WPAN, CoAP, DTLS, XMPP, MQTT, SMQTT, AMQP, LPWAN, LoRAWAN), які застосовуються на різних рівнях архітектури IoT;

– визначити найпоширеніші протоколи безпечного зв'язку IoT для запровадження в національних мережах IoT.

ОГЛЯД ЛІТЕРАТУРИ. Існує значна кількість наукових досліджень, присвячених безпеці та продуктивності протоколів зв'язку IoT. Наведемо основні з них.

У роботі А. Тріантафіллу, П. Сарігіаннідіс і Т. Д. Лагкас (2018) проаналізовано мережеві комунікаційні технології для IoT з акцентом

на протоколи інкапсуляції та маршрутизації IPv6. Науковці пропонують таксономію протоколів і досліджують внутрішні механізми їхньої роботи, що вирізняє цю працю серед інших. Обговорення також охоплює аспекти сумісності, взаємодії та конфігурації, а серед актуальних викликів виокремлено проблеми безпеки, масштабованості, мобільності й керування енергоспоживанням. Крім того, окреслено перспективні тенденції у розвитку мережевих механізмів IoT.

Опитування Г. Неббіоне та М. К. Кальцаросси (2020) присвячене вивченню безпеки протоколів прикладного рівня в середовищах IoT, зокрема тих, що стосуються обміну даними та виявлення служб. У дослідженні наголошено на складному характері ландшафту загроз, розглянуто основні проблеми, вразливості та запропоновано заходи безпеки. Результати акцентують увагу на труднощах забезпечення безпеки на прикладному рівні, зокрема на вразливості пристроїв IoT до численних ризиків, спричинених недосконалими службами безпеки у протоколах, відомими вразливостями та обмеженими ресурсами самих пристроїв.

Р. А. Рахман і Б. Шах (2016) зазначають, що IoT формує бездротову мережу, яка з'єднує інтелектуальні пристрої з інтернетом, забезпечуючи можливість інтеграції численних гаджетів і систем. Швидке розширення цього ринку викликає серйозні побоювання щодо безпеки, що, своєю чергою, стимулює створення відповідних захисних протоколів IoT.

Подібним чином у роботі Р. Крейчі, О. Гуйняка та М. Швепеша (2017) представлено огляд аспектів безпеки широко використовуваних протоколів IoT, у якому висвітлено їхні вразливості та проаналізовано еволюцію з погляду безпеки.

У дослідженні І. Хеджі, І. Шпеха та А. Шарабока (2017) подано порівняльний аналіз протоколів IoT, які застосовуються для передавання даних в обмежених мережах IoT. Учені звертають увагу на проблеми конфігурації мереж із численними фізично взаємопов'язаними пристроями.

Значний внесок у дослідження ролі IoT в обробці великих обсягів даних із різноманітних пристроїв зробили дослідниці Р. Юга та С. Чітра (2020), одночасно приділяючи увагу проблемам безпечної маршрутизації в умовах обмежених ресурсів. Основна увага в огляді зосереджена на завданнях і відкритих питаннях, що стосуються безпеки та протоколів IoT, із метою виявлення дослідницьких тенденцій та можливостей застосування інструментів моделювання для аналізу протоколів на різних рівнях архітектури IoT.

Оцінка системи безпеки IoT, проведена Б. Б. Гупти та М. Куамари (2020), представляє детальну класифікацію основних проблем у цій галузі. Автори роботи заглиблюються в такі ключові технології, як радіочастотна ідентифікація і бездротові сенсорні мережі, що мають вирішальний внесок у розвиток IoT. В огляді також досліджуються відповідні протоколи для інфраструктури IoT, акцентується увага на інструментах і платформах із відкритим кодом та завершується коротким підсумком основних проблем, можливих рішень і майбутніх напрямів досліджень у цій галузі.

Дослідження, проведене А. Аксоєм та М. Х. Гюнесом (2019), представляє автоматизовану систему, розроблену для класифікації характеристик пристроїв шляхом аналізу їхнього мережевого трафіку за допомогою одного пакету, що надходить від пристрою. Крім того, у роботі запропоновано використання генетичних алгоритмів для визначення відповідних функцій у заголовках протоколів і використання різних алгоритмів машинного навчання.

Дослідження Ж. Турньє та ін. (2021) являє собою подвійний підхід, спрямований на вирішення проблеми визначення загального методу порівняння стеків протоколів IoT на основі таких критеріїв, як діапазон, відкритість, сумісність, топологія та практика безпеки. Крім того, було запропоновано загальний спосіб опису фундаментальних атак на IoT шляхом їх класифікації на три групи: атаки, орієнтовані на пакети (пасивні й активні криптографічні атаки), атаки, зосереджені на протоколах, та атаки, зосереджені на системах. Дослідники виокремлюють спільні риси різних протоколів IoT і визначають механізми, які роблять їх уразливими до певних загроз.

Інтернет речей дає змогу об'єднувати інтелектуальні фізичні та віртуальні об'єкти, зокрема обмежені в енергоспоживанні, обчислювальних ресурсах і ємності зберігання пристрої. У роботі М. Т. Хаммі та ін. (2017) представлено надійний, спрощений і енергоефективний протокол безпеки для персональної мережі. Цей протокол забезпечує взаємну автентифікацію, шифрування й автентифікацію даних, що передаються, під час інтеграції нових пристроїв, а його ефективність підтверджено реальними тестами та оцінками продуктивності.

На думку Д. Драгомира та ін. (2016), зростання кількості пристроїв і застосунків IoT підкреслює важливість підвищення рівня безпеки

поточних протоколів і мережевих стеків. Акцент зроблено на вирішенні питань безпеки для захисту систем IoT від зловмисних атак і запобігання несанкціонованому контролю над пристроями.

Складність проєктування та впровадження політик безпеки в розгалужених мережах IoT з обмеженими ресурсами розглядається в дослідженні Х. Сардешмуха та Д. Амбаваде (2017). У ньому подано огляд стеку протоколів IoT, проведено аналіз найпоширеніших протоколів і запропоновано порівняння з орієнтацією на безпекові аспекти.

У роботі А. К. Даса, С. Зідаллі й Д. Хе (2018) окреслено систему класифікації протоколів безпеки в IoT, яка охоплює ключові елементи: керування ключами, автентифікацію користувачів і пристроїв, контроль доступу, ідентифікацію та захист конфіденційності. Дослідники також здійснили порівняльний аналіз безпекових протоколів в IoT щодо їхньої здатності забезпечувати належні функції безпеки й функціональність. Стаття завершується обговоренням майбутніх викликів у сфері безпекових протоколів для IoT.

Дослідження Г. Е. Окереке та ін. (2024) є основоположним ресурсом для глибшого розуміння та впровадження ефективних заходів безпеки в динамічному середовищі IoT-пристроїв і мережевих протоколів.

Аналіз наведених досліджень надає змогу окреслити кілька перспективних напрямів для майбутніх розвідок.

По-перше, дослідники визначають передові криптографічні методи, адаптовані до обмежених ресурсів багатьох пристроїв IoT. Розроблення легких, але надійних методів шифрування може суттєво підвищити безпеку мереж IoT.

По-друге, існує потреба у глибоких дослідженнях людського виміру безпеки IoT. Розуміння поведінки користувачів, їхнього сприйняття та взаємодії із пристроями IoT може сприяти створенню ефективніших заходів безпеки. Людські чинники, зокрема зручність використання, питання конфіденційності й обізнаність користувачів, відіграють ключову роль у загальній безпеці систем IoT. Майбутні дослідження можуть зосередитися на оптимізації цих елементів для підвищення рівня обізнаності та залученості користувачів. Крім того, важливим напрямом є дослідження у сфері стандартизації та забезпечення сумісності протоколів безпеки в екосистемі IoT.

По-третє, перспективним напрямом подальших досліджень є розроблення стандартизованих протоколів безпеки, які можуть бути універсально реалізовані, сприяючи формуванню більш захищеного та цілісного середовища IoT. Це включає співпрацю з галузевими зацікавленими сторонами й органами стандартизації для розроблення вказівок щодо безпечного впровадження IoT, сприяючи зміцненню єдиного безпекового ландшафту.

У підсумку, ця стаття орієнтована на комплексний аналіз ключових проблем, уразливостей і контрзаходів у сфері багаторівневого ландшафту безпеки IoT, наголошуючи на критичній ролі спеціалізованих протоколів зв'язку в ієрархічної архітектурі IoT. Заглиблюючись у тонкощі захищених протоколів зв'язку, дослідження робить вагомий внесок у сучасний дискурс щодо зміцнення безпеки екосистем IoT. Стандартизація та забезпечення сумісності протоколів безпеки в екосистемі IoT залишаються пріоритетними напрямами для подальших досліджень із метою створення єдиного та універсального безпекового простору в екосистемі IoT.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. Методологія науково-технічного дослідження кібербезпеки пристроїв IoT на основі впровадження спеціалізованих протоколів зв'язку включає кілька кроків, описаних нижче.

Першим кроком у процесі дослідження було детальне визначення проблем. Основна увага зосереджена на безпеці передачі даних між пристроєм і пунктом призначення. Через обмеженість ресурсів пристрої IoT не можуть підтримувати традиційні протоколи безпеки транспортного рівня, як-от TLS, необхідні для захисту зв'язку. Тому застосовують, наприклад, протокол датаграм – DTLS. Він уважається складним протоколом, і не всі пристрої IoT мають достатньо ресурсів для його підтримки. У таких умовах можливо використовувати шлюз як посередника між пристроєм IoT і кінцевим пунктом призначення. Тобто дані можуть бути оброблені в більш безпечній формі у шлюзі перед передачею через інтернет, але їхній вміст залишається незахищеним до моменту обробки й надсилання. Це робить дані вразливими до атак, якщо шлюз буде зламано зловмисником. Безпека на рівні каналу передачі може захистити саму передачу, однак якщо неавторизована особа отримає доступ до бездротової мережі, вона потенційно зможе перехопити дані.

Другим кроком дослідження є визначення цілей на основі проблем, встановлених на попередньому етапі. Ці цілі – це вимоги, необхідні для їх вирішення. Можливими вимогами є: забезпечення безпеки даних між пристроєм і призначенням; захист даних між пристроєм і

шлюзом; захист даних між шлюзом і пунктом призначення; захист даних, що проходять через шлюз; ефективна й своєчасна передача даних без втрат.

Використання шлюзу розділяє процес передачі даних на дві частини: передача даних між пристроєм і шлюзом, а також передача даних між шлюзом і місцем призначення в інтернеті. Кожна із цих частин потребує різних механізмів безпеки, які мають відповідати можливостям пристроїв.

Для забезпечення безпеки даних між пристроями IoT і вебсервером необхідно забезпечити конфіденційність даних між джерелом і одержувачем.

Дані, що передаються через інтернет, мають бути надійно захищені. Шлюзи можуть забезпечити додатковий рівень захисту. Щоб захистити конфіденційні дані, слід застосовувати надійні та правильно реалізовані стандарти шифрування. Якщо зловмисник отримує контроль над шлюзом, він може отримати доступ до даних, які обробляються. Тому шлюз є критичним об'єктом у системі безпеки, і дані мають бути захищені навіть під час їх обробки.

Третім кроком є аналіз вимог для розроблення плану із захисту системи. Це ітеративний процес, у якому на кожному етапі відбувається перегляд вимог і цілей, щоб переконатися, що захист системи йде за планом.

Четвертий крок методології включає впровадження та оцінку. На цьому етапі аналізується безпека даних на кожному етапі передачі. Висновки ґрунтуються на оцінці ефективності системи кібербезпеки, а також визначаються переваги й недоліки використаних протоколів безпеки.

П'ятий крок – це представлення результатів дослідження у вигляді звіту, а також їх обговорення та аналіз. Отримані результати і міркування стануть корисними рекомендаціями для подальших досліджень у цій сфері. Очікується, що в межах цього етапу буде виявлено нові напрями, які потребують подальшого опрацювання, що дозволить іншим дослідникам розвивати отримані напрацювання.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. Інтеграція речей в інтернет є складною, оскільки вони можуть мати обмежені характеристики: пам'ять, обчислювальну потужність і енергетичні ресурси. Більшість продуктів спочатку розроблялися як закриті пропрієтарні рішення, які були несумісні із пристроями інших виробників. Проте поточна тенденція спрямована на стандартизовані протоколи (Клімушин, 2025).

Вимоги безпеки IoT класифікують за п'ятьма категоріями: безпека мережі, управління ідентифікацією та доступом, конфіденційність, довіра та стійкість (Dragomir et al., 2016).

Вимоги до безпеки мережі охоплюють конфіденційність, цілісність, автентифікацію походження, актуальність і доступність.

Вимоги до управління ідентифікацією та доступом включають автентифікацію, авторизацію, відкликання та звітність. Управління ідентифікацією та доступом є важливою проблемою в системах IoT через складні відносини між об'єктами (пристроями, послугами, постачальниками послуг, власниками та користувачами).

Вимоги до конфіденційності стосуються захисту даних, анонімності та псевдоможливості зв'язування. Конфіденційність є важливою проблемою в системах IoT, оскільки користувачі потребують захисту своїх особистих даних, що містять інформацію про їхні звички, взаємодію та місцезнаходження.

Вимоги до довіри охоплюють довіру до даних і до об'єктів, а також такі аспекти, як довіра до обробки, довіра до з'єднання та довіра до системи загалом.

Вимоги до стійкості мають особливе значення для великомасштабних систем IoT, які є вразливими до атак і збоїв через складність і різноманітність апаратного та програмного забезпечення. Системи виявлення та запобігання вторгненням забезпечують захист від зловмисних атак і відновлення нормального функціонування після порушення стійкості.

Дослідники пропонують різні стандартні архітектури IoT, проте не існує універсальної архітектури, яку б загалом підтримувала наукова спільнота. Найпростішою та загальноприйнятою архітектурою є архітектура, яка включає три основні рівні: рівень сприйняття, мережевий рівень і прикладний рівень (Hassija et al., 2019).

Найнижчий рівень – *рівень сприйняття* – охоплює фізичні пристрої IoT, зокрема датчики, приводи та інші компоненти. Основне його завдання – фіксувати параметри навколишнього середовища для збору відповідних даних. Атаки на цьому рівні мають на меті вивести пристрої з ладу, підвищити їхнє енергоспоживання або викрасти інформацію (Liao, Shuai, Wang, 2018).

Установлення зв'язку між кінцевими пристроями IoT і серверами належить до функцій другого – *мережевого* – рівня стеку протоколів. Коли інформація надходить до нього з рівня сприйняття, він може виконувати аналіз даних. Фішинг, атаки на відмову в обслуговуванні,

розподілені атаки на відмову в обслуговуванні, атаки на маршрутизацію, несанкціонований доступ та інші типові атаки можуть бути успішними проти цього рівня (Choudhary, Kesswani, 2019).

На останньому – *прикладному* – рівні реалізується широкий спектр IoT-застосунків, таких як «розумні міста», «розумні будинки», «розумні електромережі», охорона здоров'я, громадська безпека та багато інших. Основні загрози тут пов'язані із крадіжкою даних, порушенням конфіденційності та безпекою.

В інших системах поверх прикладного рівня розміщуються додатки бізнес-рівня, які керують архітектурою IoT і відповідають за безпеку даних користувачів, фінансове адміністрування та керування програмами. Основна мета цього рівня – запобігти будь-яким спробам викрадення даних.

На кожному рівні системи IoT застосовуються численні протоколи (див. рис. 1). Деякі з них подібні до протоколів традиційних IT-систем, проте інші є унікальними для комунікаційної архітектури IoT. Йдеться про протоколи: IEEE 802.15.4, NFC, Zigbee, BLE, RPL, 6L0WPAN, CoAP, DTLS, XMPP, MQTT, SMQTT, AMQP, LPWAN, LoRAWAN (Choudhary, Meena, 2022).

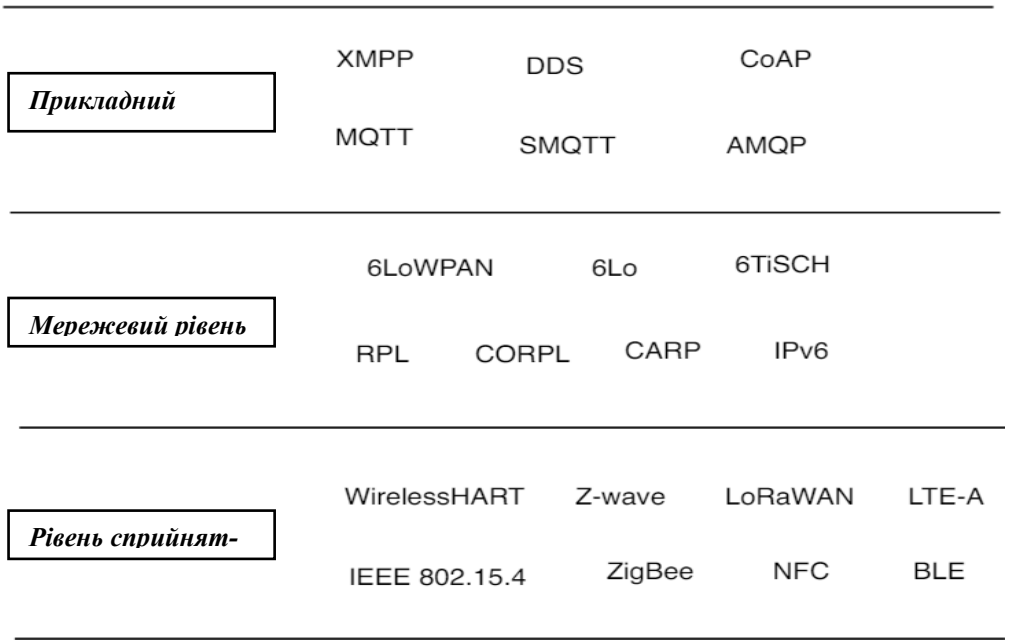

Рис. 1. Протоколи передачі даних у середовище IoT

Стандарти рівня сприйняття охоплюють протоколи фізичного рівня (*Physical Layer*, PHY) та керування доступом до середовища (*Media Access Control*, далі - MAC), які поєднуються в більшості стандартів.

1. Стандарт IEEE 802.15.4 – це стандарт каналу передачі даних, який зазвичай використовується на рівні MAC. Він визначає формат кадру, заголовки, адреси призначення і джерела, а також спосіб встановлення зв'язку між вузлами. Стандарт забезпечує зв'язок на невеликі відстані з низьким енергоспоживанням і малою пропускною здатністю, що робить його особливо придатним для пристроїв IoT з обмеженими ресурсами. Метод кодування, який використовується у стандарті IEEE 802.15.4, має вбудовану надмірність, яка підвищує надійність з'єднання, дозволяє ідентифікувати втрати даних і здійснювати повторну передачу втрачених пакетів. Він використовує синхронізацію часу та перемикання каналів, щоб забезпечити високу надійність і низьку вартість зв'язку в каналах передачі даних.

Особливості стандарту IEEE 802.15.4 можна підсумувати так: використання структур слот-фрейма для визначення стану вузлів (прийом, передавання, режим сну); планування передавання відповідно до заданого алгоритму централізованого керівного вузла; синхронізація взаємодії між вузлами; частотне перемикання каналів у бездротовому середовищі, що зменшує вплив перешкод і багатопроменевого завмирання (Salman, Jain, 2017a; Salman, Jain, 2017б).

Стандарт IEEE 802.15.4 надає послуги безпеки на рівні MAC, які, незважаючи на те, що були розроблені для захисту зв'язку на канальному рівні, є цінними для підтримки

механізмів безпеки, реалізованих на вищих рівнях стеку протоколів. Це зумовлено можливістю ефективного використання криптографії на апаратному рівні сенсорних платформ із застосуванням стандарту симетричного шифрування AES (*Advanced Encryption Standard*) (Granjal, Monteiro, Silva, 2015).

Стандарт IEEE 802.15.4 передбачає використання зіркоподібної та однорангової топологій для забезпечення зв'язку між вузлами, де передані дані повинні проходити через координаційний вузол або центр. Цей стандарт визначає рівень керування доступом до середовища MAC і фізичний рівень (PHY), нижні рівні моделі мережі взаємозв'язку відкритих систем (*Open Systems Interconnection*, OSI), які використовуються в усьому світі та підтримуються групою IEEE 802.15 (Karthik et al., 2018).

На рисунку 2 показано стек стандарту IEEE 802.15.4 (Rani, Gill, 2019). Тут IEEE 802.2 використовується як логічний контроль зв'язку (*Logical Link Control*, LLC), який взаємодіє з підрівнями конвергенції. Логічний контроль зв'язку є верхньою частиною канального рівня (*Data Link Layer*, DLL) у моделі *Open Systems Interconnection*. Стандарт IEEE 802.15.4 є добре відомим технічним стандартом для низькошвидкісної бездротової персональної мережі (*Low-Rate Wireless Personal Area Network,* LR-WPAN).

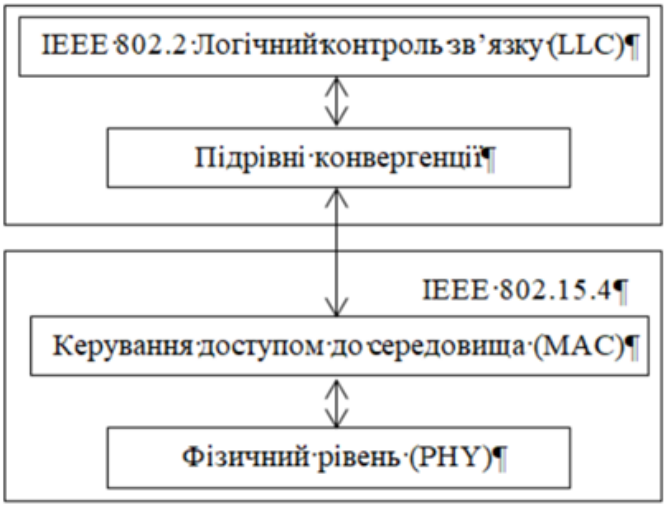

Рис. 2. Стек стандарту IEEE 802.15.4

2. Мобільні пристрої можуть спілкуватися на невеликій відстані (всього кілька міліметрів) за допомогою зв'язку ближнього поля (*Near-Field Communication*, далі – NFC), що є різновидом бездротового зв'язку з мінімальним радіусом дії. Для передавання даних достатньо з'єднати два пристрої, оснащені NFC, і розмістити їх поруч – це дає змогу миттєво передавати дані у будь-якому форматі. Основою цієї технології є радіочастотна ідентифікація (*Radio Frequency Identification*, далі – RFID).

Передача даних між двома NFC-пристроями здійснюється через коливання магнітного поля. Існує два режими роботи – активний і пасивний. В активному режимі обидва пристрої генерують магнітне поле. У пасивному – лише один із них відповідає за його створення, а другий використовує модуляцію навантаження для передавання даних.

З метою економії енергії пристрої з живленням від батареї часто використовують пасивний режим. Однією з переваг обмеженої зони дії NFC є її придатність для безпечних транзакцій, зокрема платежів, оскільки для обміну даними пристрої мають бути в безпосередній близькості. На відміну від RFID, NFC забезпечує двосторонній зв'язок. Саме тому переважна більшість сучасних мобільних телефонів підтримує цю технологію.

Промисловість широко використовує технологію RFID для контролю запасів, логістичних потоків, відстеження продукції та керування ланцюжком поставок (Radan, Samimi, Moeni, 2018).

3. Персональні мережі Zigbee (Pooja, Khaparkar, Sahu, 2018) були розроблені альянсом Zigbee за стандартом IEEE 802.15.4. Їхньою основною метою є сприяння створенню комунікаційних рішень із високою надійністю, економністю та низьким загальним енергоспоживанням. Зв'язок між пристроями Zigbee можливий лише на відстані від кількох до приблизно 100 метрів. Крім того, цей стандарт передбачає набір вимог до складових елементів і функціональних можливостей мережевого та прикладного рівнів.

Розширені функції цього стандарту охоплюють шифрування даних, автентифікацію, маршрутизацію та пересилання даних. Таким чином, протоколи за стандартом Zigbee забезпечують підвищений рівень безпеки. Найчастіше цей стандарт використовується в бездротових сенсорних мережах. У сітчастій топології будь-який вузол може обмінюватися даними з іншим за умови перебування в межах допустимого радіуса дії.

Версії Zigbee можуть підтримувати енергозбирання в умовах відсутності батареї та підключення до мережі змінного струму. Застосунки за стандартом Zigbee містять такі функції, як дистанційне керування, інтелектуальний моніторинг енергії, автоматизація будівель, інтелектуальна охорона здоров'я, інтелектуальне освітлення, периферійні пристрої та пристрої (клавіатура, миша, сенсорні панелі тощо), а також багато інтелектуальних мережевих служб. Це надійна технологія, яку використовують у всьому світі. Водночас згідно з численними дослідженнями (Mu, Han, 2017) проблемою залишається споживання електроенергії, що потребує подальшої оптимізації для підвищення задоволеності користувачів. Технологія зв'язку 5G розгортається в інтелектуальних пристроях і терміналах, які потенційно можуть бути інтегровані з мережею Zigbee для покращення продуктивності передавання даних.

Zigbee може функціонувати в зіркоподібній, деревоподібній або сітчастій топології залежно від ситуації. Топологія визначає реалізацію механізму маршрутизації, який слід використовувати. Zigbee також має додаткові властивості: здатність ідентифікації, підтримку вузлів, які приєднуються до мережі та виходять із неї, короткі 16-бітні адреси, маршрутизацію з кількома переходами.

Безпека мережі Zigbee забезпечується за допомогою двох ключів шифрування: мережевого ключа і ключа посилання. Мережевий ключ використовується для захисту широкомовного зв'язку. Це 128-бітний ключ, спільний для всіх пристроїв у мережі. Пристрій може отримати його двома способами: шляхом попереднього встановлення або транспортування ключа. Ключ посилання застосовується для захисту одноадресного зв'язку. У цьому разі лише два пристрої мають спільний 128-бітний ключ. Ключ посилання також може бути отриманий або шляхом попереднього встановлення, або транспортуванням.

4. За розробку технології *Bluetooth Low Energy* (далі – BLE) відповідає організація Bluetooth Special Interest Group. Ця технологія споживає значно менше енергії та має значно менший радіус дії порівняно з іншими альтернативними технологіями.

Стек протоколів, що використовується у BLE, подібний до того, який застосовується у класичному Bluetooth. Він поділяється на дві частини: контролер і хост. Обидва компоненти взаємодіють між собою через стандартизований інтерфейс хост-контролера (Dragomir et al., 2016). У порівнянні з класичним Bluetooth, BLE є значно ефективнішим з погляду енергоспоживання та вартості реалізації пристрою. Архітектура BLE включає фізичний рівень (PHY), канальний рівень, контроль логічного зв'язку та протокол адаптації (*Logical Link Control and Adaptation Protocol*, L2CAP). Протоколи верхнього рівня та атрибути мультиплексуються.

У звичайному Bluetooth з'єднання залишається активним навіть у разі відсутності передавання чи отримання даних. Крім того, технологія дозволяє використовувати 79 каналів даних, кожен з яких має смугу пропускання 1 МГц. Натомість BLE використовує лише 40 доріжок, має пропускну здатність каналу 2 МГц, що вдвічі більше, ніж у стандартного Bluetooth. Завдяки невеликому розміру пакета та швидкості передавання BLE протокол здатен працювати з мінімальними потребами в робочому циклі. Крім того, стек протоколів BLE полегшує зв'язок на основі IP. У порівнянні з Zigbee, BLE демонструє приблизно у 2,5 рази вищу енергоефективність.

5. Протокол маршрутизації для мережі з низьким енергоспоживанням і втратами (*Routing Protocol for Low-Power and Lossy Networks*, далі – RPL) – це новий вид технології маршрутизації, розроблений спеціально для гаджетів IoT. Цей протокол застосовується в мережах 6L0WPAN. Використовуючи вузли, які вже є в мережі, і цільову функцію як механізм зв'язування, RPL генерує спрямований ациклічний граф, орієнтований на призначення (*Destination Oriented Directed Acyclic Graph*, далі – DODAG). Він використовує адресу IP версії 6 як засіб самоопису. Ще однією особливістю DODAG є те, що кожен вузол запам'ятовує свої сусідні вузли і топологія мережі ранжується від найнижчого до найвищого.

Керуючі повідомлення для міжмережевого IP (*Internet Control Message Protocol for the Internet Protocol Version 6*, ICMPv6) RPL відомі за своїми абревіатурами: інформаційний об'єкт DODAG (далі – DIO), запит інформації DODAG (DIS) і цільовий рекламний об'єкт (далі – DAO) / підтвердження цільового рекламного об'єкта (далі – DAO-ACK). Повідомлення DIO використовуються для зберігання та оновлення інформації про шляхи маршрутизації. Повідомлення

DAO, коли їх читають зверху вниз, публікують дані маршрутизації, що надсилаються між дочірнім вузлом і вузлом-приймачем. Наявні вузли надають повідомлення DAO у формі повідомлень DIO, щоб допомогти з додаванням нового вузла до мережі. Існує спеціальний тип повідомлення під назвою DAO-ACK, який можна використовувати для підтвердження отримання повідомлення DAO.

6. Протокол 6L0WPAN використовується для бездротових персональних мереж із низьким енергоспоживанням, який дає змогу передавати пакети (*Internet Protocol Version 6*, далі – IPv6) через канали зв'язку IEEE 802.15.4 і забезпечує IP-з'єднання в мережевих системах з обмеженими ресурсами (Devasena, 2016).

Протокол 6L0WPAN – це рівень адаптації, який використовується між мережевим рівнем (IPv6) і канальним рівнем (IEEE 802.15.4 MAC) для маршрутизація між віддаленими пристроями. Рівень адаптації виконує фрагментацію для пересилання пакетів IPv6 через радіозв'язок IEEE 802.15.4.

Особливістю 6L0WPAN є підтримка 64-бітної або 16-бітної адреси, стиснення заголовків IPv6 і протоколу користувацьких датаграм (*User Datagram Protocol*, далі – UDP), орієнтація на мережі з низьким енергоспоживанням за допомогою BLE, підтримка одноадресної, широкомовної та багатоадресної передачі, а також фрагментація (Devasena, 2016). Протокол 6L0WPAN є відкритим протоколом мережі IoT і може слугувати альтернативою дорогим технологіям Wi-Fi.

7. Протокол обмеженого застосування (*Constrained Application Protocol*, далі – CoAP) є полегшеним протоколом, призначеним для використання з пристроями з низьким енергоспоживанням і в мережах з обмеженими ресурсами, таких, які зазвичай використовуються в системах IoT. Передбачається, що він стане більш простою та ефективною альтернативою протоколу передачі гіпертексту (*Hypertext Transfer Protocol*, далі – HTTP) для пристроїв з обмеженою обчислювальною потужністю, пам'яттю та часом автономної роботи. Протокол CoAP побудований поверх протоколу UDP та надає набір методів для виявлення ресурсів, управління ними, спостереження, а також підтримку асинхронного зв'язку та кешування.

Завдяки низьким накладним витратам та простоті реалізації CoAP стає дедалі популярнішим у застосунках IoT та, як очікується, відіграватиме важливу роль у подальшому розвитку цієї галузі. Це стандарт для більшості програм IoT. Протокол CoAP – не просто альтернатива HTTP, а вдосконалене рішення, адаптоване до специфіки обмежених середовищ.

Формат даних EXI (*Efficient XML Interchanges*) використовує двійкові дані, що робить його значно ефективнішим порівняно зі стандартними форматами передачі гіпертексту HTML або розширюваної мови розмітки (*Extensible Markup Language,* далі – XML), які використовують звичайний текст. Деякі додаткові можливості включають: вбудоване стиснення заголовків, виявлення ресурсів, автоматичне налаштування, асинхронний обмін повідомленнями, контроль перевантаження та підтримку багатоадресної передачі. Усі ці функції є стандартними.

У протоколі CoAP передбачено чотири типи повідомлень: непідтверджувані, підтверджувані, повідомлення скидання і повідомлення підтвердження. Підтверджувані повідомлення гарантують, що дані, надіслані через протокол UDP, досягнуть пункту призначення без втрат і пошкоджень. Крім того, для додаткового захисту використовується протокол датаграм безпеки транспортного рівня (*Datagram Transport Layer Security*, далі – DTLS). Протокол DTLS базується на потоковому протоколі TLS і забезпечує безпечну взаємодію для клієнт-серверних програм, запобігаючи фальсифікації, підслуховуванню та підробці повідомлень.

Архітектура CoAP складається переважно з двох підрівнів: обміну повідомленнями та запиту / відповіді. Повідомлення передаються через ці підрівні. Підрівень обміну повідомленнями забезпечує надлишкове виявлення й надійну доставку повідомлення, яке базується на передачі повідомлень про зупинку та очікування. Підрівень запит / відповідь відповідає за зв'язок. Цей підрівень може використовувати як синхронні, так і асинхронні відповіді.

8. Розширюваний протокол обміну повідомленнями та присутності (*Extensible Messaging and Presence Protocol*, далі – XMPP) – це відкрита стандартна технологія протоколу обміну повідомленнями. Спочатку його було розроблено для миттєвого обміну повідомленнями між користувачами мережі Інтернет із забезпеченням основних функцій безпеки, зокрема наскрізного шифрування, автентифікації та сумісності (Ramirez, Pedraza, 2017). Цей протокол є текстовим і ґрунтується на розширюваній мові розмітки XML, який може реалізувати як публікацію-підписку, так і взаємодію клієнт-сервер. Хоча XMPP підтримує модель клієнт-сервер для взаємодії, але також є нові розширення, які можуть увімкнути загальну модель публічної підписки. Завдяки цим розширенням XMPP може створювати

теми та публікувати інформацію. Зв'язок клієнт-сервер у XMPP здійснюється через потоки XML. Обмін даними здійснюється у формі XML-структурованих строф або тегів.

Протокол XMPP також відомий як стандарт обміну миттєвими повідомленнями (*Instant Messaging*, IM). Серед прикладних можливостей XMPP – відеодзвінки, телеконференції та спілкування в чаті. Це безпечний протокол, який є більш придатним для IoT-середовищ порівняно з моделлю запит / відповідь у CoAP. XMPP вважається одним із найефективніших протоколів для платформ IoT.

9. Протокол телеметрії черги повідомлень (*Message Queue Telemetry Transport*, далі - MQTT) – це один із найкращих легких протоколів, що працює на архетипі публікації / підписки. Протокол є придатним для пристроїв з обмеженими ресурсами та мережевих з'єднань із неідеальними умовами, такими як висока затримка та низька пропускна здатність (Dizdarevic et al., 2018). Це простий структурований протокол із високою надійністю. У порівнянні з іншими надійними протоколами обміну повідомленнями, MQTT має легший заголовок і потребує менше енергії. Завдяки своїй простоті та наявності невеликого заголовка повідомлення його часто рекомендують для зв'язку в IoT. Цей протокол не схожий на протокол типу запит / відповідь – він функціонує поверх транспортних протоколів.

Протокол MQTT використовує шаблон публікації / підписки для гнучкості переходу та впровадження. Це ідеальний легкий протокол обміну повідомленнями. MQTT – це протокол, орієнтований на повідомлення, розроблений переважно для зв'язку «пристрій – пристрій» (*Machine-to-Machine*, далі – M2M) і застосунків віддаленої телеметрії (Tukade, Banakar, 2018).

Протокол MQTT включає чотири основні компоненти: 1) брокер – головний компонент, що працює як сервер і використовується для моніторингу даних між віддаленими пристроями та датчиками. Він дозволяє пристроям автоматично з'єднуватися з іншими пристроями, використовуючи три основні рівні якості обслуговування (*Quality of Service*, QoS); 2) тема – створює інформацію про назву на основі деяких тем; 3) видавець; 4) підписник (Sonawala, Tank, Patel, 2017). Зазвичай клієнтами є пристрої, які здатні публікувати повідомлення. Клієнти знають про брокерів, до яких він підключається, і коли він виконує роль підписника, він повинен знати про тему. Щоб отримати відповідне повідомлення, клієнт може підписатися на певну тему. Інші клієнти також можуть підписатися на ту саму тему, щоб отримувати оновлення від брокерів із кожним надходженням повідомлення. Брокери повинні класифікувати дані видавців за темами і відправляти тим підписникам, які цікавляться відповідними темами. Протокол MQTT призначений для встановлення вбудованого зв'язку між проміжним програмним забезпеченням і застосунками, а також комунікаціями та мережами (Salman, Jain, 2017б).

10. Безпечний MQTT (*Secure Message Queue Telemetry Transport*, далі – SMQTT) (Salman, Jain, 2017б) є захищеним розширенням протоколу MQTT. Протокол SMQTT використовує легкі атрибути шифрування та був розроблений для покращення функції безпеки MQTT. Найважливішою особливістю SMQTT є широкомовне шифрування за допомогою секретного головного ключа відповідно до алгоритму генерації ключів, обраного розробником. При цьому не існує стандартизованого алгоритму для генерації ключів і шифрування.

11. Розширений протокол черги повідомлень (*Advanced Message Queuing Protocol*, далі – AMQP) – це протокол обміну повідомленнями сеансового рівня. Його було розроблено для потреб промисловості та бізнесу з метою запропонувати непатентовані рішення для передавання великої кількості повідомлень. Основні можливості доставлення повідомлень, які надає AMQP, включають: точка – точка, зберігання та пересилання. Протоколи MQTT і AMQP використовують схожі методи передавання повідомлень. AMQP функціонує поверх транспортного протоколу TCP і відповідає архітектурі видавець / підписник.

Протокол AMQP було створено для забезпечення взаємодії між широким колом доменних застосунків і систем. Його сумісність є ключовою перевагою, оскільки дозволяє обмінюватися повідомленнями між різними платформами та мовами програмування. Це робить AMQP особливо корисним у гетерогенних системах (Dizdarevic et al., 2018). Протокол AMQP працює подібно до систем електронної пошти або сервісів миттєвих повідомлень. Його архітектура складається з мережевих протоколів, які визначають взаємодію між трьома основними компонентами: виробником, споживачем і брокером.

Обробка повідомлень у AMQP є автономною, а вміст повідомлень – непрозорим. AMQP – це протокол проміжного програмного забезпечення, який використовується для обміну повідомленнями у розподілених програмних середовищах. Він також забезпечує абстрагування та спрощення комунікаційних застосунків,

гарантуючи надійність у роботі з їхніми різними об'єктами.

12. Технологія глобальної мережі низького енергоспоживання (*Low Power Wide Area Network*, далі – LPWAN) (Mu, Han, 2017) була розроблена для інтеграції великої кількості пристроїв в IoT. Ця технологія є альтернативою стільниковим мережам малого радіуса дії, пропонуючи пристрої з великою дальністю зв'язку, нижчою вартістю і тривалішим часом роботи акумулятора. Глобальна мережа великого радіусу дії (*Long Range Wide Area Network*, далі – LoRAWAN) була розроблена шляхом оптимізації LPWAN для низької вартості, меншого енергоспоживання, широкого радіусу покриття і ємності. Технологію LoRAWAN розроблено та підтримується LoRAWAN Alliance – некомерційною відкритою асоціацією.

Мережі LoRAWAN використовують топологію «зірка»: кінцеві пристрої надсилають повідомлення до шлюзів, а ті, своєю чергою, ретранслюють повідомлення на сервер. Уся інформація, що передається з кінцевого IoT-пристрою, захищена наскрізним шифруванням із застосуванням двох рівнів криптографічного захисту: 128-бітного мережевого ключа та 128-бітного ключа сесії програми.

До сильних сторін технології LoRaWAN належать: висока дальність передавання порівняно з іншими бездротовими технологіями; добра проникаюча здатність у міському середовищі; швидке та просте розгортання мережі; тривалий термін служби акумуляторів; легкість масштабування; низька вартість базових станцій і кінцевих пристроїв. Як і в будь-якої іншої системи, у LoRaWAN є й недоліки: значна затримка передавання даних від кінцевих пристроїв і невисока пропускна здатність.

Отже, існує значна кількість спеціалізованих протоколів безпечного зв'язку для IoT, які відрізняються рівнем продуктивності. До найпоширеніших протоколів, рекомендованих для впровадження в національних мережах IoT, належать такі.

1. Відкритий стандартний протокол AMQP, що використовується у проміжному програмному забезпеченні, орієнтований на повідомлення, забезпечує безпеку, взаємодію та зв'язок навіть за відсутності одночасної доступності систем. Його широко застосовують у таких сферах, як мікросервісна архітектура, інтеграція систем, обробка подій і IoT-рішення. Завдяки гнучкості та надійності AMQP забезпечує ефективну взаємодію між розподіленими системами.

2. Стандартний протокол BLE підтримується широким спектром пристроїв, що спрощує їхню взаємодію між собою. Ця бездротова технологія малого радіусу дії використовується для потокового аудіо в персональних мережах із низьким енергоспоживанням і малим радіусом дії.

Технологія BLE стала популярною для широкого спектра застосувань, зокрема у гаджетах, медичних приладах, промисловій та побутовій автоматизації. Її широко використовують під час розроблення IoT-пристроїв, які потребують низького енергоспоживання та бездротового зв'язку на короткій відстані. Це одна з ключових технологій у таких пристроях, як фітнес-трекери й «розумні» годинники. Медичні прилади, зокрема глюкометри й пульсометри, також застосовують BLE для бездротового зв'язку зі смартфонами та іншими пристроями

3. Протокол прикладного рівня CoAP призначений для IoT-пристроїв з обмеженими ресурсами. Його розроблено для роботи в мережах із низькою пропускною здатністю та обмеженою обчислювальною потужністю, що забезпечує ефективну передачу даних між пристроями. Це спрощена версія протоколу HTTP. CoAP підтримує засоби безпеки через налаштування протоколу датаграм безпеки транспортного рівня DTLS.

Цей протокол активно застосовують у проєктах легкої комунікації: у «розумних» містах, де численні малопотужні пристрої, такі як вуличні ліхтарі й датчики паркування, повинні зв'язуватися з центральними серверами; у сільському господарстві – для підключення датчиків вологості ґрунту та систем автоматизованого зрошення; у моніторингу довкілля – для збирання екологічних даних із віддалених датчиків; у домашній автоматизації – для забезпечення ефективної взаємодії між датчиками та пристроями без надмірного споживання енергії.

4. Мережевий протокол LoRaWAN, що вирізняється низьким енергоспоживанням, використовує фізичну широкосмугову модуляцію LoRa. Він дає змогу вирішувати ключові завдання IoT для бізнесу: збір даних із великої кількості пристроїв на значній території; подовження терміну служби кінцевих пристроїв; економію часу та коштів завдяки швидкому розгортанню мережі, її легкому масштабуванню та можливості дистанційного обслуговування. Застосування технології LoRaWAN у національних мережах дає змогу ефективно розв'язувати різні завдання, зокрема: об'єднувати дані з усіх приладів обліку ресурсів в єдину систему; здійснювати моніторинг протікань, поломок, задимленості; контролювати

стан довкілля; відстежувати місце перебування та переміщення працівників; керувати вуличним освітленням; створювати оптимальні умови для тварин та рослин у теплицях, на полях, у силосних ямах; організовувати контроль за механізмами та вузлами тощо.

5. Протокол MQTT (SMQTT), що використовує архітектуру публікації-підписки для забезпечення зв'язку M2M для пристроїв з обмеженими ресурсами та в мережах із низькою пропускною здатністю, змінним рівнем затримки та нестабільним з'єднанням. Завдяки відкритому коду, його широко використовують для підключення IoT-пристроїв. MQTT застосовують у промисловому IoT, «розумних» будинках, автомобілях та дистанційному моніторингу пацієнтів у медицині. Протокол ідеально підходить для розподілених комунікацій «один до багатьох» для створення систем управління виробництвом у режимі реального часу.

В інтелектуальних енергомережах MQTT дає змогу передавати показники лічильників у реальному часі, що забезпечує точне нарахування оплат для споживачів. У точному землеробстві цей протокол забезпечує надійний контроль за датчиками вологості ґрунту й аналіз стану культур навіть за нестабільного підключення. Завдяки гарантованій доставці повідомлень фермери своєчасно отримують сповіщення про посуху чи шкідників, що допомагає зберегти врожай і ресурси.

Для моніторингу технічного стану пристроїв MQTT забезпечує безперервне дистанційне спостереження, миттєво передаючи операторам дані про вібрацію, температуру та інші параметри. Це дозволяє виявляти зношені компоненти та запобігати аварійним зупинкам.

У системах білінгу MQTT підвищує точність і прозорість обліку. Надійна доставка повідомлень і виявлення дублікатів покращують обробку платіжної інформації у телекомунікаційних і комунальних компаніях.

6. Протокол XMPP – відкритий стандарт для обміну повідомленнями в реальному часі. Підходить для M2M-зв'язку у спрощеному проміжному програмному забезпеченні та для маршрутизації XML-даних, підтримує обмін структурованими даними в реальному часі між кількома об'єктами в мережі для розгортання споживчих та інтелектуальних IoT.

Цей протокол застосовують у багатьох сферах, зокрема для миттєвих повідомлень, інформування про присутність, спільної роботи, соціальних мереж, телеметрії, дистанційного керування та інших напрямів. XMPP став основою для низки популярних месенджерів і комунікаційних платформ.

Серед основних функцій безпеки XMPP: шифрування, автентифікація, контроль доступу, наскрізне шифрування, захист міжсерверного зв'язку, робота з брандмауерами, мережевий захист, фільтрація повідомлень, контроль вмісту, аудит і ведення журналу, а також підтримка розширень безпеки. Під час розроблення застосунків на основі XMPP необхідно дотримуватися найкращих практик для забезпечення оптимальної продуктивності, безпеки та сумісності.

7. Протокол Zigbee широко застосовується в системах автоматизації, зокрема в «розумних» будинках, промисловому моніторингу, медичному обладнанні та побутовій електроніці. Він ідеально підходить для застосунків, які потребують енергоефективного бездротового з'єднання між пристроями, що працюють на батарейках.

Головна перевага стандарту Zigbee – низьке енергоспоживання, що дає змогу пристроям працювати на батареях упродовж тривалого часу. Окрім того, Zigbee підтримує мережі з великою кількістю пристроїв (до 65 000), які можуть бути розташовані на значній відстані одне від одного. Це робить його ефективним рішенням для «розумних» будинків, енергоощадних промислових мереж та інших IoT-систем. Стандарт Zigbee також включає засоби безпеки, зокрема шифрування та автентифікацію, що допомагає захищати мережу від несанкціонованого доступу та зламів.

Загалом проведене обговорення ґрунтується на стеку протоколів за різними алгоритмами зв'язку IoT. Механізми, що формують цей стек, забезпечують стабільний інтернет-зв'язок для обмежених сенсорних пристроїв IoT із низьким енергоспоживанням.

ВИСНОВКИ. У статті представлено систематичний огляд літератури та здійснено комплексний аналіз комунікаційних технологій і спеціалізованих протоколів, спрямованих на забезпечення безпеки середовищ IoT. Розглянуто архітектуру системи, передові технології, а також проблеми безпеки та конфіденційності. Розуміння основ кібербезпеки в контексті IoT вимагає розпізнавання типів пристроїв, їхніх вразливостей і потенційних загроз, з якими вони можуть стикатися.

Протоколи IoT – це стандартизовані мови, що полегшують зв'язок між пристроями, серверами та хмарними платформами IoT. Вони є основою безперебійної взаємодії в межах екосистеми IoT. У зв'язку з мільйонами взаємопов'язаних пристроїв, які передають конфіденційні дані, компанії стикаються із серйозними викликами у сфері безпеки IoT, здатними поставити під загрозу їхню діяльність.

Вимоги безпеки IoT класифікують за п'ятьма категоріями: безпека мережі, управління ідентифікацією, конфіденційність, довіра та стійкість. З огляду на ці вимоги дослідники запропонували різні стандартні архітектури IoT. Проте на сьогодні не існує єдиної універсальної архітектури, яка мала б загальне визнання. Найпростішою та загальноприйнятою архітектурою є архітектура, яка включає три основні рівні: рівень сприйняття, мережевий рівень і прикладний рівень. Для забезпечення безпечної взаємодії між пристроями IoT на кожному із цих рівнів використовуються як традиційні, так і спеціалізовані протоколи зв'язку.

У дослідженні визначено найпоширеніші протоколи безпечного зв'язку IoT і представлено практику їх застосування з урахуванням таких критично важливих параметрів, як продуктивність, обсяг пам'яті, пропускна здатність, швидкість передавання даних, вартість, потужність і енергоспоживання. Також подано порівняння їхніх переваг і недоліків.

Заглиблюючись у тонкощі функціонування захищених протоколів зв'язку, дослідження робить внесок у сучасний дискурс про зміцнення безпеки національних екосистем IoT. Стандартизація та сумісність протоколів безпеки залишаються важливими напрямами для подальших досліджень з метою створення єдиного, узгодженого й надійного ландшафту безпеки в середовищі IoT.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Клімушин П. С. Проблемні аспекти стандартизації кібербезпеки Інтернету речей. *Право і безпека*. 2025. № 1 (96). С. 53–66. DOI: https://doi.org/10.32631/pb.2025.1.05.

2. 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.

3. Aksoy A., Gunes M. H. Automated IoT Device Identification using Network Traffic // IEEE International Conference on Communications (Shanghai, China, 20–24 May 2019). Shanghai, 2019. DOI: https://doi.org/10.1109/ICC.2019.8761559.

4. Alam M., Khan S., Shakil K. A. Internet of Things (IoT): Concepts and Applications. Switzerland : Springer, 2020. 532 p. DOI: https://doi.org/10.1007/978-3-030-37468-6.

5. Choudhary S., Kesswani N. A Survey: Intrusion Detection Techniques for Internet of Things. *International Journal of Information Security and Privacy*. 2019. Vol. 13, No. 1. Pp. 86–105. DOI: https://doi.org/10.4018/IJISP.2019010107.

6. Choudhary S., Meena G. Internet of Things: Protocols, Applications and Security Issues. *Procedia Computer Science*. 2022. Vol. 215. Pp. 274–288. DOI: https://doi.org/10.1016/j.procs.2022.12.030.

7. Das A. K., Zeadally S., He D. Taxonomy and analysis of security protocols for the Internet of Things. *Future Generation Computer Systems*. 2018. Vol. 89. Pp. 110–125. DOI: https://doi.org/10.1016/j.future.2018.06.027.

8. Devasena C. L. IPv6 Low Power Wireless Personal Area Network (6LoWPAN) for Networking Internet of Things (IoT) – Analyzing its Suitability for IoT. *Indian Journal of Science and Technology*. 2016. Vol. 9, No. 30. DOI: https://doi.org/10.17485/ijst/2016/v9i30/98730.

9. Dizdarevic J., Carpio F., Jukan A. Masip-Bruin X. A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. *ACM Computing Surveys*. 2018. Vol. 51, No. 6. DOI: https://doi.org/10.1145/3292674.

10. Dragomir D., Gheorghe L., Costea S., Radovici A. A Survey on Secure Communication Protocols for IoT Systems // International Workshop on Secure Internet of Things (Heraklion, Greece, 26–30 September 2016). Heraklion, 2016. DOI: https://doi.org/10.1109/SIoT.2016.012.

11. Gerodimos A., Maglaras L, Kantzavelou I., Ayres N. IoT: Communication Protocols and Security Threats. *Electrical and Electronic Engineering.* 2022. Vol. 1. DOI: https://doi.org/10.20944/preprints202111.0214.v2.

12. Granjal J., Monteiro E., Silva J. S. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*. 2015. Vol. 17, No. 3. Pp. 1294–1312. DOI: https://doi.org/10.1109/COMST.2015.2388550.

13. Gupta B. B., Quamara M. An overview of the Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience*. 2020. Vol. 32, No. 21. DOI: https://doi.org/10.1002/cpe.4946.

14. Hammi M. T., Livolant E., Bellot P., Serhrouchni A., Minet P. A lightweight IoT security protocol // 1st Cyber Security in Networking Conference (Rio de Janeiro, Brazil, 18–20 October 2017). Rio de Janeiro, 2017. DOI: https://doi.org/10.1109/CSNET.2017.8242001.

15. Hassija V., Chamola V., Saxena V., Jain D., Goyal P., Sikdar B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access*. 2019. Vol. 7. Pp. 82721–82743. DOI: https://doi.org/10.1109/ACCESS.2019.2924045.

16. Heđi I., Špeh I., Šarabok A. IoT network protocols comparison for the purpose of IoT-constrained networks // 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (Opatija, Croatia, 22–26 May 2017). Opatija, 2017. DOI: https://doi.org/10.23919/MIPRO.2017.7973477.

17. Karthik B. N., Parameswari L. D., Harshini R., Akshaya A. Survey on IOT & Arduino Based Patient Health Monitoring System. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 2018. Vol. 3, No. 1. Pp. 1414–1417.

18. Krejčí R., Hujňák O., Švepeš M. Security survey of the IoT wireless protocols // 25th Telecommunication Forum (Belgrade, Serbia, 21–22 November 2017). Belgrade, 2017. DOI: https://doi.org/10.1109/TELFOR.2017.8249286.

19. Liao C. H., Shuai H. H., Wang L. C. Eavesdropping prevention for heterogeneous Internet of Things systems // 15th IEEE Annual Consumer Communications & Networking Conference (Las Vegas, USA, 12–15 January 2018). Las Vegas, 2018. DOI: https://doi.org/10.1109/CCNC.2018.8319297.

20. Maglaras L., Ferrag M. A., Derhab A., Mukherjee M., Janicke H., Rallis S. Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures. *Transactions on Security and Safety.* 2019. Vol. 5, No. 16. DOI: https://doi.org/10.4108/eai.15-10-2018.155856.

21. Mu J., Han L. Performance analysis of the ZigBee networks in 5G environment and the nearest access routing for improvement. *Ad Hoc Networks.* 2017. Vol. 56, No. 4. DOI: https://doi.org/10.1016/j.adhoc.2016.10.006.

22. Nebbione G., Calzarossa M. C. Security of IoT application layer protocols: Challenges and findings. *Future Internet*. 2020. Vol. 12, No. 3. DOI: https://doi.org/10.3390/fi12030055.

23. Okereke G. E., Mathew D. E., Ukeoma P. E., Uzo B. C., Umaru A. A., Dibiaezue N. F. IoT Device Security and Network Protocols: A Survey on the Current Challenges, Vulnerabilities, and Countermeasures. *International Advanced Research Journal in Science, Engineering and Technology.* 2024. Vol. 11, Iss. 7. DOI: https://doi.org/10.17148/IARJSET.2024.11701.

24. Pooja K., Khaparkar S., Sahu P. A Literature Survey on Zigbee / IEEE 802.15.4 System Implementation. *International Journal of Current Engineering and Scientific Research*. 2018. Vol. 2, Iss. 4. Pp. 2503–2509. DOI: https://doi.org/10.31142/ijtsrd14574.

25. Radan A., Samimi H., Moeni A. A new lightweight authentication protocol in IoT environment for RFID tags. *International Journal of Engineering and Technology*. 2018. Vol. 4, No. 7. Pp. 344–351. DOI: https://doi.org/10.14419/ijet.v7i4.7.23028.

26. Rahman R. A., Shah B. Security analysis of IoT protocols: A focus in CoAP // 3rd MEC International Conference on Big Data and Smart Cities (Muscat, Oman, 15–16 March 2016). Muscat, 2016. DOI: https://doi.org/10.1109/ICBDSC.2016.7460363.

27. Ramirez J., Pedraza C. Performance analysis of communication protocols for Internet of things platforms // IEEE Colombian Conference on Communications and Computing (Cartagena, Colombia, 16–18 August 2017). Cartagena, 2017. DOI: https://doi.org/10.1109/ColComCon.2017.8088198.

28. Rani D., Gill N. S. Review of Various IoT Standards and Communication Protocols. *International Journal of Engineering Research and Technology.* 2019. Vol. 12, No. 5. Pp. 647–657.

29. Salman T., Jain R. A Survey of Protocols and Standards for Internet of Things. *Advanced Computing and Communications*. 2017a. Vol. 1, No. 1. DOI: https://doi.org/10.48550/arXiv.1903.11549.

30. Salman T., Jain R. Networking Protocols and Standards for Internet of Things // Internet of Things and Data Analytics Handbook / ed. by H. Geng. New York, John Wiley & Sons, 20176. Pp. 215–238. DOI: https://doi.org/10.1002/9781119173601.

31. Sardeshmukh H., Ambawade D. Internet of Things: Existing protocols and technological challenges in security // International Conference on Intelligent Computing and Control (Coimbatore, India, 23–24 June 2017). Coimbatore, 2017. DOI: https://doi.org/10.1109/I2C2.2017.8321835.

32. Sonawala N. M., Tank B., Patel H. IoT Protocol based environmental data monitoring // International Conference on Computing Methodologies and Communication (Erode, India, 18–19 July 2017). Erode, 2017. DOI: https://doi.org/10.1109/ICCMC.2017.8282629.

33. Tournier J., Lesueur F., Le Mouël F., Guyon L., Ben-Hassine H. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things*. 2021. Vol. 16, No. 4. DOI: https://doi.org/10.1016/j.iot.2020.100264.

34. Triantafyllou A., Sarigiannidis P., Lagkas T. D. Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends. *Wireless Communications and Mobile Computing*. 2018. Vol. 2. DOI: https://doi.org/10.1155/2018/5349894.

35. Tukade T. M., Banakar R. M. Data Transfer Protocols in IoT-An overview. *International Journal of Pure and Applied Mathematics*. 2018. Vol. 118, No. 16. Pp. 121–138.

36. Yugha R., Chithra S. A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications*. 2020. Vol. 169. DOI: https://doi.org/10.1016/j.jnca.2020.102763.

Надійшла до редакції: 07.04.2025

Прийнята до опублікування: 10.06.2025

REFERENCES

1. Aksoy, A., & Gunes, M. H. (2019, May 20–24). *Automated IoT Device Identification using Network Traffic* [Conference presentation abstract]. IEEE International Conference on Communications, Shanghai, China. https://doi.org/10.1109/ICC.2019.8761559.

2. Alam, M., Khan, S., & Shakil, K. A. (2020). *Internet of Things (IoT): Concepts and Applications*. Springer. https://doi.org/10.1007/978-3-030-37468-6.

3. Choudhary, S., & Kesswani, N., (2019). A Survey: Intrusion Detection Techniques for Internet of Things. *International Journal of Information Security and Privacy, 13*(1), 86–105. https://doi.org/10.4018/IJISP.2019010107.

4. Choudhary, S., & Meena, G. (2022). Internet of Things: Protocols, Applications and Security Issues. *Procedia Computer Science, 215*, 274–288. https://doi.org/10.1016/j.procs.2022.12.030.

5. Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for the Internet of Things. *Future Generation Computer Systems, 89*, 110–125. https://doi.org/10.1016/j.future.2018.06.027.

6. Devasena, C. L. (2016). IPv6 low power wireless personal area network (6LoWPAN) for networking Internet of Things (IoT) – Analyzing its suitability for IoT. *Indian Journal of Science and Technology, 9*(30). https://doi.org/10.17485/ijst/2016/v9i30/98730.

7. Dizdarevic, J., Carpio, F., Jukan, A., & Masip-Bruin, X. (2018). A survey of communication protocols for Internet-of-Things and related challenges of fog and cloud computing integration. *ACM Computing Surveys, 51*(6). https://doi.org/10.1145/3292674.

8. Dragomir, D., Gheorghe, L., Costea, S., & Radovici, A. (2016, September 26–30). *A Survey on Secure Communication Protocols for IoT Systems* [Conference presentation abstract]. International Workshop on Secure Internet of Things, Heraklion, Greece. https://doi.org/10.1109/SIoT.2016.012.

9. Gerodimos, A., Maglaras, L, Kantzavelou, I., & Ayres, N. (2022). IoT: Communication Protocols and Security Threats. *Electrical and Electronic Engineering, 1*. https://doi.org/10.20944/preprints202111.0214.v2.

10. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials, 17*(3), 1293–1312. https://doi.org/10.1109/COMST.2015.2388550.

11. Gupta, B. B., & Quamara, M. (2020). An overview of the Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience, 32*(21). https://doi.org/10.1002/cpe.4946.

12. Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P. (2017). *A lightweight IoT security protocol* [Conference presentation abstract]. 1st Cyber Security in Networking Conference, Rio de Janeiro, Brazil. https://doi.org/10.1109/CSNET.2017.8242001.

13. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access, 7*, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045.

14. Heđi, I., Špeh, I., & Šarabok, A. (2017). *IoT network protocols comparison for the purpose of IoT-constrained networks* [Conference presentation abstract]. 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia. https://doi.org/10.23919/MIPRO.2017.7973477.

15. Karthik, B. N., Parameswari, L. D., Harshini, R., & Akshaya, A. (2018). Survey on IOT & Arduino Based Patient Health Monitoring System. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3*(1), 1414–1417.

16. Klimushyn, P. S. (2025). Problematic aspects of IoT cybersecurity standardisation. *Law and Safety, 1*(96), 53–66. https://doi.org/10.32631/pb.2025.1.05.

17. 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.

18. Krejčí, R., Hujňák, O., & Švepeš, M. (2017). *Security survey of the IoT wireless protocols* [Conference presentation abstract]. 25th Telecommunication Forum, Belgrade, Serbia. https://doi.org/10.1109/TELFOR.2017.8249286.

19. Liao, C. H., Shuai, H. H., & Wang, L. C. (2018). *Eavesdropping prevention for heterogeneous Internet of Things systems* [Conference presentation abstract]. 15th IEEE Annual Consumer Communications & Networking Conference, Las Vegas, USA. https://doi.org/10.1109/CCNC.2018.8319297.

20. Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2019). Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures. *Transactions on Security and Safety, 5*(16). https://doi.org/10.4108/eai.15-10-2018.155856.

21. Mu, J., & Han, L. (2017). Performance analysis of the ZigBee networks in 5G environment and the nearest access routing for improvement. *Ad Hoc Networks, 56*(4). https://doi.org/10.1016/j.adhoc.2016.10.006.

22. Nebbione, G., & Calzarossa, M. C. (2020). Security of IoT application layer protocols: Challenges and findings. *Future Internet, 12*(3). https://doi.org/10.3390/fi12030055.

23. Okereke, G. E., Mathew, D. E., Ukeoma, P. E., Uzo, B. C., Umaru, A. A., & Dibiaezue, N. F. (2024). IoT Device Security and Network Protocols: A Survey on the Current Challenges, Vulnerabilities, and Countermeasures. *International Advanced Research Journal in Science, Engineering and Technology, 11*(7). https://doi.org/10.17148/IARJSET.2024.11701.

24. Pooja, K., Khaparkar, S., & Sahu, P. (2018). A Literature Survey on Zigbee / IEEE 802.15.4 System Implementation. *International Journal of Current Engineering and Scientific Research, 2*(4), 2503–2509. https://doi.org/10.31142/ijtsrd14574.

25. Radan, A., Samimi, H., & Moeni, A. (2018). A new lightweight authentication protocol in IoT environment for RFID tags. *International Journal of Engineering and Technology, 4*(7), 344–351. https://doi.org/10.14419/ijet.v7i4.7.23028.

26. Rahman, R. A., & Shah, B. (2016). *Security analysis of IoT protocols: A focus in CoAP* [Conference presentation abstract]. 3rd MEC International Conference on Big Data and Smart Cities, Muscat, Oman. https://doi.org/10.1109/ICBDSC.2016.7460363.

27. Ramirez, J., & Pedraza, C. (2017). *Performance analysis of communication protocols for Internet of things platforms* [Conference presentation abstract]. IEEE Colombian Conference on Communications and Computing, Cartagena, Colombia. https://doi.org/10.1109/ColComCon.2017.8088198.

28. Rani, D., & Gill, N. S. (2019). Review of Various IoT Standards and Communication Protocols. *International Journal of Engineering Research and Technology, 12*(5), 647–657.

29. Salman, T., & Jain, R. (2017a). A Survey of Protocols and Standards for Internet of Things. *Advanced Computing and Communications, 1*(1). https://doi.org/10.48550/arXiv.1903.11549.

30. Salman, T., & Jain, R. (2017b). Networking Protocols and Standards for Internet of Things. In H. Geng (Ed.), *Internet of Things and Data Analytics Handbook* (pp. 215–238). John Wiley & Sons. https://doi.org/10.1002/9781119173601.

31. Sardeshmukh, H., & Ambawade, D. (2017). *Internet of Things: Existing protocols and technological challenges in security* [Conference presentation abstract]. International Conference on Intelligent Computing and Control, Coimbatore, India. https://doi.org/10.1109/I2C2.2017.8321835.

32. Sonawala, N. M., Tank, B., & Patel, H. (2017). *IoT Protocol based environmental data monitoring* [Conference presentation abstract]. International Conference on Computing Methodologies and Communication, Erode, India. https://doi.org/10.1109/ICCMC.2017.8282629.

33. Tournier, J., Lesueur, F., Le Mouël, F., Guyon, L., & Ben-Hassine, H. (2021). A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things, 16*(4). https://doi.org/10.1016/j.iot.2020.100264.

34. Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends. *Wireless Communications and Mobile Computing, 2*. https://doi.org/10.1155/2018/5349894.

35. Tukade, T. M., & Banakar, R. M. (2018). Data Transfer Protocols in IoT-An overview. *International Journal of Pure and Applied Mathematics, 118*(16), 121–138.

36. Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. *Journal of Network and Computer Applications, 169*. https://doi.org/10.1016/j.jnca.2020.102763.

Received the editorial office: 7 April 2025

Accepted for publication: 10 June 2025

PETRO SERHIIOVYCH KLIMUSHYN,
Kharkiv National University of Internal Affairs,
Educational and Scientific Institute No. 4,
Department of Combating Cybercrime;
ORCID: https://orcid.org/0000-0002-1020-9399,
e-mail: klimushyn@ukr.net

COMMUNICATION TECHNOLOGIES AND SPECIALISED COMMUNICATION PROTOCOLS FOR ENSURING CYBERSECURITY OF THE INTERNET OF THINGS

Internet of Things devices are characterised by limited resources in terms of power, processing, memory and bandwidth. As a result, traditional protocols relating to network operations and security cannot be implemented in their current form in the specific environment of the Internet of Things.

Standardisation is necessary for the organisation of IoT interaction, because without established regulations, precise instructions and global standards, the industry will eventually face serious compatibility and security issues. In addition, many IoT devices process sensitive data that they can autonomously collect and distribute to other devices or the network. There is a need for stronger data protection measures and stricter controls for IoT devices that authenticate and interact on the network. Protecting IoT devices and communication protocols has become a priority in our increasingly connected world.

It is noted that the analysis of the security of IoT communication technologies using specialised communication protocols across networks with different topologies, communication ranges and bandwidths is a pressing issue, as the number of security and privacy breaches in the IoT ecosystem is growing, which is constantly expanding in various sectors of the economy and human life with the introduction of billions of heterogeneous smart devices. In addition, many Internet of Things networks cover a wide range of communication protocols, some of which may not have reliable security features, making them vulnerable to attacks.

The term "communication technology" is used to define communication protocols at each level of the Internet of Things platform architecture. In an effort to provide a better understanding of the architecture and use of Internet of Things technologies, the taxonomy presented in the article facilitates the effective separation of relevant Internet of Things technologies into channel-level protocols, network encapsulation protocols, and routing protocols according to their standards.

The study may encourage scientists and professionals to develop new and more effective network protocols based on the current gaps and shortcomings discussed in the article.

Keywords: *Internet of Things, Internet of Things architecture, Internet of Things security, Internet of Things security protocols, Internet of Things communication protocols, network protocols, cellular communication.*

Цитування (ДСТУ 8302:2015): Клімушин П. С. Комунікаційні технології та спеціалізовані протоколи зв'язку для забезпечення кібербезпеки Інтернету речей. *Право і безпека*. 2025. № 2 (97). С. 52–68. DOI: https://doi.org/10.32631/pb.2025.2.05.

Citation (APA): Klimushyn, P. S. (2025). Communication Technologies and Specialised Communication Protocols for Ensuring Cybersecurity of the Internet of Things. *Law and Safety, 2*(97), 52–68. https://doi.org/10.32631/pb.2025.2.05