відні локальні мережі в більшості випадків будуються на базі технології Ethernet і оптоволокна, а бездротові - на базі технології Wi-Fi. Для організації Глобальної мережі (Wide Area Network, WAN) використовуються технології WiMax, LTE і ін. В останні два роки з'явилися технології зв'язку для підключення пристроїв з низьким енергоспоживанням до глобальної мережі – LPWAN. Тож детально розглянемо кожну із технологій, проаналізувавши основні їх переваги, недоліки та особливості застосування.

Технологія Bluetooth LE. Bluetooth - це бездротова технологія, що забезпечує передачу даних на невеликих відстанях і дає змогу пристроям, які використовують цю технологію, обмінюватися даними [3,8]. Bluetooth дозволяє спілкуватися таким пристроям тоді, коли вони перебувають в радіусі до 10 метрів один від одного.

Великою перевагою Bluetooth LE є низьке енергоспоживання і енергоспоживання в режимі сну, надмале пікове енергоспоживання.

Пристрої, які використовують Bluetooth LE споживають менше енергії і здатні передавати дані в 50 разів швидше, в порівнянні з Bluetooth-пристроями попередніх поколінь. Для комфортного використання в областях домашніх розваг, охорони здоров'я та охоронних систем ця версія Bluetooth дає підтримку широкого діапазону додатків і дозволяє зменшити розмір кінцевого пристрою.

Пристрої BLE працюють в діапазоні 2,4 ГГц. Основними областями застосування BLE є пристрої забезпечення безпеки, управління електроприладами і відображення показань, датчики на батарейках, домашні медичні прилади, спортивні тренажери.

Технологія Wi-Fi. Wireless LAN стандарту WiFi 802.11 розроблялася для надання бездротового широкосмугового доступу до мереж передачі даних на високих швидкостях. Стек протоколів стандарту IEEE 802.11 складається з фізичного рівня PHY і канального рівня з підрівнями управління доступом до середовища MAC і логічної передачі даних LLC [9].

За допомогою Wi-Fi можна розгорнути мережу без прокладки кабелю, мати доступ до мережі мобільних пристроїв. В межах Wi-Fi зони, в мережу Інтернет можуть виходити кілька користувачів з комп'ютерів, ноутбуків, планшетів, телефонів і т. д.

Бездротова локальна обчислювальна мережа предметів WiFi підключена до Internet за допомогою роутера. Слід зазначити, що для побудови локальних бездротових обчислювальних мереж предметів Wi-Fi Alliance створив нову специфікацію IEEE 802.11s, яка забезпечує технологію побудови пористих мереж.

Крім того, для IoT створений і новий стандарт Wi-Fi HaLow (специфікація IEEE 802.11ah) [3] з низьким енергоспоживанням. Даний вид зв'язку функціонуватиме в діапазоні менше 1 Ггц, специфікації IEEE 802.11ah. Для підключення Wi-Fi HaLow буде використовуватися неліцензована частота 900 МГц. Це помітно збільшить проникаючу здатність сигналу в міській забудові, а радіус її дії буде набагато більше, ніж у сучасного бездротового стандарту, - до 1 кілометра. У той же час платою за «далекобійність» є мала потужність сигналу. Пропускна здатність Wi-Fi HaLow буде набагато нижче, ніж максимум Wi-Fi 802.11ac (7 Гбіт / с), передбачувана швидкість: 50 кбіт / с - 18 Мбіт / с [10].

Технологія ZigBee (6LoWPAN). ZigBee – технологія, заснована на стандарті IEEE 802.15.4 і призначена для створення бездротових персональних мереж (WPAN) з використанням малопотужних радіопередавачів малих розмірів. Технологія ZigBee націлена на додатки, які потребують більшого часу автономної роботи від батареї і більшої безпеки, при передачі даних на невеликих швидкостях [11, 12].

Специфікація ZigBee орієнтована на програми, що вимагають гарантованої безпечної передачі даних при відносно невеликих швидкостях і можливості три-

валої роботи мережевих пристроїв від автономних джерел живлення (батарей). Вона забезпечує невисоке споживання енергії та передачу даних зі швидкістю до 250 Кбіт / с на відстань до 75 метрів в умовах прямої видимості [13].

Пристрої ZigBee можуть переходити від сплячого режиму роботи до активної за 15 мілісекунд або менше, що значно менше в порівнянні з технологією Bluetooth, для якої затримка при переході від сплячого до активного режиму досягає близько 3-х секунд.

Основна особливість технології ZigBee полягає в тому, що вона при малому енергоспоживанні підтримує не тільки прості топології мережі («точка-точка», «дерево» і «зірка»), а й самоорганізуючу і самовідновлюючу порожнисту (mesh) топологію з ретрансляцією і маршрутизацією повідомлень . Крім того, специфікація ZigBee забезпечує простоту розгортання, обслуговування та модернізації.

Технологія Z-Wave. Z-Wave - це перший відкритий бездротовий стандарт домашньої автоматизації (системи «розумний» будинок), в основі якої лежить коміркова (mesh) мережа [10]. Цей стандарт використовує частоту 908 МГц і просувається в даний час на ринок в якості більш дешевої альтернативи технології ZigBee.

На відміну від Wi-Fi і інших стандартів передачі даних IEEE 802.11, призначених в основному для великих потоків інформації, стандарт Z-Wave працює в діапазоні частот до 1 ГГц і оптимізований для передачі простих керуючих команд (наприклад, включити / виключити, змінити гучність, яскравість і т.д.). Вибір низького радіочастотного діапазону для Z-Wave обумовлюється малою кількістю можливих джерел електромагнітних полів (на відміну від завантаженого діапазону 2,4 ГГц, в якому доводиться вдаватися до заходів, що зменшують можливі перешкоди від працюючих різних побутових бездротових пристроїв - Wi-Fi, ZigBee, Bluetooth) . Також іншими перевагами стандарту можна відзначити мале споживання енергії, низьку вартість виробництва і вбудовування модулів Z-Wave в різні побутові пристрої.

Швидкість передачі даних в мережі становить 9,6 кбіт / с або 40 кбіт / с з повною сумісністю. Радіус дії приблизно 30 метрів в умовах прямої видимості, в приміщенні зменшується в залежності від форми і матеріалу стін, а також від виду антени.

Технологія Z-Wave призначена для домашньої автоматизації та володіє аналогічним принципом побудови, але меншою функціональністю. Використовує малопотужні і мініатюрні радіочастотні модулі, які вбудовуються в побутову електроніку і різні системи, такі як освітлення, опалення, контроль доступу, розважальні системи і побутову техніку.

Очевидним недоліком Z-Wave є відсутність масштабованості, необхідної при збільшенні числа підтримуваних функцій в домашніх і промислових мережах.

Технологія LoRaWAN. Мережа LoRa (англ. Long Range) стає все більш популярним рішенням для концепції IoT. LoRaWAN - це «умовно глобальна» мережа, яка призначена для мереж дальнього радіусу дії, з метою передачі даних телеметрії різних приладів обліку (датчиків води, газу і т.д.) на далекі відстані. Приклад реалізації LoRa-мережі наведений на рис. 4 [14].

Рис. 4. Реалізація мережі LoRaWAN

Вона складається з кінцевих пристроїв (nodes), які відправляють дані на концентратори (gateway). Кожен концентратор має доступ до мережі Інтернет, і відправляє прийняті дані на сервер, який в свою чергу розсилає їх підписаним клієнтам.

Технологія LoRaWAN являє собою мережу розмірів району, або навіть цілого міста. Мережа LoRaWAN має просту архітектуру типу "зірка" (від англ. Star) без ретрансляторів і mesh-зв'язків та призначена для збору даних з великої кількості датчиків, які рівномірно розташовані на значній площі. Вузлам мережі характерне низьке енергоспоживання (до 10 років роботи від звичайних батарей AA), невисока швидкість обміну даними, велика дальність зв'язку (15 км в сільській місцевості і 5км в щільній міській забудові) і низька вартість кінцевого обладнання.

Протокол 6LoWPAN. 6LoWPAN (IPv6 Low-Power Wireless Personal Area Network) – стандарт, який забезпечує взаємодію малих бездротових мереж з мережами IP по протоколу IPv6 з малим енергоспоживанням [15].

Стандарт 6LoWPAN підключає безліч пристроїв до «хмари». Мала потужність, IP-адресовані вузли та підтримка великих пористих мереж роблять цю бездротову технологію хорошим вибором для додатків Інтернету речей (IoT). Повне ім'я - «IPv6 over LowPower Wireless Personal Area Networks» означає «передача пакетів IPv6 поверх малопотужних бездротових персональних мереж» [15]. Передача даних в стандарті 6LoWPAN має на увазі використання субгігагерцового діапазону і забезпечує швидкість передачі від 50 до 200 Кбіт / с на відстань до 800 метрів. Отже, 6LoWPAN є мережевою технологією або рівнем адаптації, який дозволяє ефективно передавати пакети IPv6 в невеликих фреймах канального рівня, визначених в бездротовому стандарті IEEE 802.15.4.

Перш за все, мережі 6LoWPAN є підмережами IPv6-мереж, тобто вони можуть взаємодіяти з іншими мережами і вузлами IP-мережі, але не є транзитними для її мережевого трафіку.

6LoWPAN полягає в тому, що він був спочатку розроблений, щоб підтримувати малопотужні бездротові мережі 2,4 ГГц, побудовані на базі IEEE 802.15.4, але тепер цей стандарт адаптований і використовується в безлічі інших середовищ мережевої передачі, включаючи бездротові мережі в діапазонах нижче 1 ГГц, Smart Bluetooth, передачу даних по лініях електропередачі (PLC) і малопотужні мережі Wi-Fi [16].

Таким чином, бачимо деякі переваги та недоліки безпроводових техноголій, які можуть бути використані в концепції IoT, а також їх області потенційного застосування (табл. 1).

Таблиця 1. Порівняння основних технологій концепції IoT

Технічні характеристики	**Wi-Fi**	**Wi-Fi HaLow**	**ZigBee**	**LoRaWAN**	**Z-Wave**	**Bluetooth LE**
Стандарт	IEEE 802.11	IEEE 802.11 ah	IEEE 802.15.4	LoRaWAN	Z-Wave	Bluetooth 4.0
Частота	2,4 ГГц, 5 ГГц	900 МГц	915 МГц / 2,4 Ггц	863-870 МГц	900 МГц	2,4 ГГц
Дальність дії	До 100 м	До 1 км	100 м / Mesh	2-5 км в місті; до 15 км поза містом	30 м / Mesh	80 м
Швидкість передачі	7 Гбіт/с	50 кбіт/с – 18 Мбіт/с	250 кбіт/с	290 біт/с - 50 Кбіт/с	10-100 кбіт/с	< 1 Мбіт/с
Енергоспоживання	Високе	Понижене	Низьке	Низьке	Низьке	Низьке
Масштабованість	Так	Так	Так	Так	Обмежено	Так
Діапазон ISM	Так	Так	Так	Так	Так	Так
Аутентифікація	Так	Так	Так	Так	Так	Проблематично
E2E шифрування	Так	Так	Так	Так	Так	Так
Вартість обладнання	Висока	Висока	Низька	Низька	Висока	Низька
Місцезнаходження сенсора відомо	Так	Так	-	Так	-	Ні
Повна двоспрямованість	Так	Так	Так	Так, в залежності від режиму	Так	Так
Підтримка сенсорів, які рухаються між хабами	Так	Так	Так, mesh	Так	Так, mesh	Так

Протоколи мережевого (IP, протоколи маршрутизації), транспортного (TCP, UDP, SCTP) рівнів моделі OSI, які представлені на рис. 2 та задіяні в обміні даними в концепції IoT, детально розглянуті в ряді вітчизняних та закордонних праць [6,11,12,18], а також в рекомендаціях ITU [6] та відповідних RFC [5, 17]. Тому в даній роботі дані протокли не будемо піддавати детальному аналізу. Сконцентруємося лише на протоколах прикладного рівня моделі OSI. Прикладний рівень відповідає за форматування даних. Він також перевіряє, що дані транспортуються за оптимальною для застосування схемою.

До найпоширеніших протоколів прикладного рівня в концепції IoT відносять:

- REST/HTTP;
- MQTT;
- XMPP;
- AMQP;
- CoAP.

Протокол HTTP. На прикладному рівні в Інтернеті широко використовується протокол – HTTP, який є символьно-орієнтованим клієнт-серверним протоколом, що запускається поверх TCP [18,21]. HTTP використовує XML - текстовий мову з великим об'ємом службової інформації. Тому не оптимально використовувати HTTP в багатьох системах 6LoWPAN. Однак HTTP все ще може бути дуже корисним для зв'язку між 6LoWPAN і Інтернетом.

Протокол MQTT. MQTT (Message Queuing Telemetry Transport) - легкий і простий протокол обміну повідомлення-

ми, який реалізує модель «публікація / підписка» (publish / subscribe) і призначений для зв'язку комп'ютеризованих пристроїв, подключѐнних до локальної або глобальної мережі, між собою і різними громадськими чи приватними веб- сервісами [20].

Його завдання - замінити технології, використовувані різними компаніями і стати таким же стандартом обміну даними в мережі Інтернет, як протокол HTTP.

Протокол MQTT спочатку був створений для датчиків, які відстежують стан труб, проте пізніше сфера його діяльності була розширена і він знайшов своє застосування в безлічі вбудованих рішень, в тому числі в смартфонах. Так соціальна мережа Facebook застосовує цей протокол для обміну повідомленнями (Facebook Messenger).

У мережі на базі протоколу MQTT розрізняють 3 об'єкти (рис. 5) [17]:

1) видавець (publisher) - MQTT-клієнт, який при виникненні певних подій передає інформацію про нього до брокера;

2) брокер (broker) - MQTT-сервер, який приймає інформацію від видавців і передає її відповідним передплатникам, в складних системах може виконувати також різні операції, пов'язані з аналізом і обробкою даних, що надійшли;

3) передплатник (subscriber) - MQTT-клієнт, який після підписки у відповідного брокера більшу частину часу «слухає» його і постійно готовий до прийому і обробки вхідного повідомлення від брокера. Протокол працює за схемою передплатник / видавець, тобто всі повідомлення від клієнта до клієнта проходять через центрального брокера.

Протокол спроектований спеціально для мобільних додатків "інтернету речей", де часто необхідна робота від батарей в умовах повільної і нестабільної мережі. Таким чином, MQTT використовує мінімальну кількість трафіку і висуває дуже скромні вимоги до заліза. На практиці підійде майже будь-який контролер, на якому може бути піднято TCP стек.

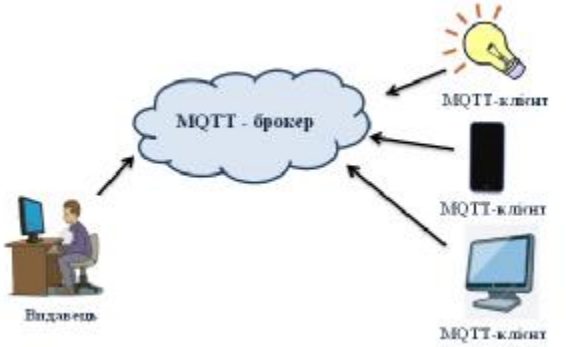

Рис. 5. Основна структура роботи протокола MQTT

Протокол MQTT має ряд переваг, порівняно з протоколом HTTP: менші накладні витрати на передачу даних і менша смуга пропускання. Для своєї роботи він не вимагає постійного з'єднання між клієнтом і сервером (як у випадку HTTP). MQTT також добре адаптований до роботи по каналах зв'язку з низькою пропускною здатністю.

Протокол XMPP. Протокол XMPP (Extensible Messaging and Presence Protocol) - розширюваний протокол обміну повідомленнями та інформацією про присутність [18]. Він був розроблений для системи миттєвого обміну повідомленнями для зв'язку між людьми за допомогою текстових повідомлень (рис. 6) [18].

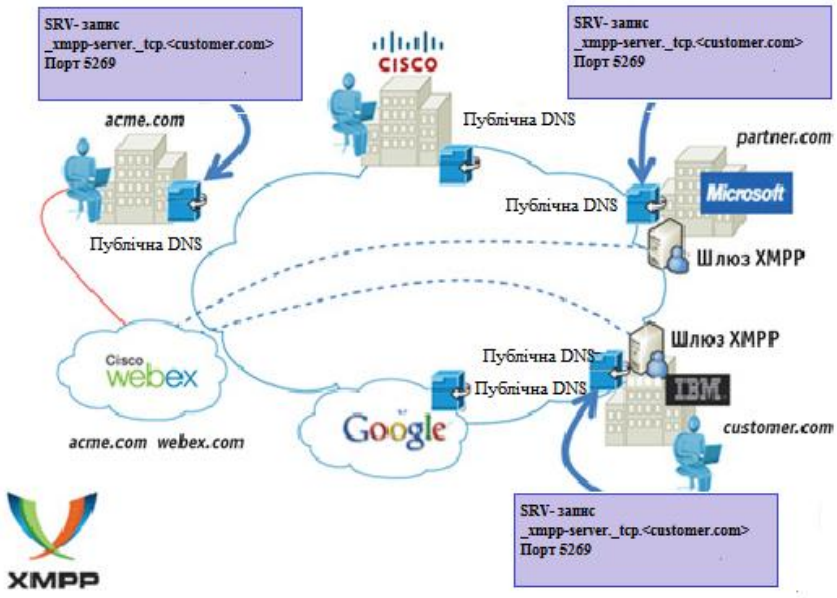

Рис. 6. Обмін текстовими повідомленнями між точками доступу в протоколі XMPP

Стосовно Інтернету речей, XMPP забезпечує простий спосіб адресації пристроїв. Для ідентифікації користувачів використовуються запам'ятовуються ідентифікатори JID, за форматом схожі на адреси електронної пошти (наприклад, username@jabber.ru). У протоколі XMPP застосовується текстовий формат XML. XMPP працює на основі протоколутранспортного рівня TCP і забезпечує асинхронний та синхронний алгоритм обміну повідомленнями. Його перевагою є метод адресації виду name@domain.com, який допомагає з'єднувати користувачів в величезному просторі Інтернету. XMPP підтримує різні комунікаційні моделі (запит-відповідь, публікація-підписка і інші).

Адресація XMPP особливо зручна у випадках, коли дані передаються між віддаленими, найчастіше незалежними точками, наприклад в разі взаємодії двох абонентів. Цей протокол не володіє високою швидкістю. Фактично, в більшості реалізацій цього протоколу використовується метод опитування або перевірки доповнень тільки на вимогу. За допомогою XMPP, наприклад, можливе підключення домашнього термостата до Web-серверу для отримання до нього доступу з телефону. Сильними сторонами цього протоколу є також безпека і масштабованість, що робить його ідеальним для додатків Інтернету речей з орієнтацією на споживача.

Протокол AMQP. AMQP (Advanced Message Queuing Protocol, або вдосконалений протокол організації черги повідомлень), який іноді розглядають як протокол IoT [19]. Як випливає з назви, AMQP обслуговує виключно черги. Він пересилає транзакційні сполучення між серверами. Цей протокол, в якості орієнтованого на повідомлення проміжного програмного забезпечення, був створений для банківської галузі і здатний обробляти тисячі організованих в чергу транзакцій.

У протоколі AMQP велику увагу приділено боротьбі з втратою повідомлень. Різні комунікаційні лінії – від постачальників контенту до комутаторів каналів і від списків черговості до користувачів – використовують протокол TCP, який забезпечує високонадійне двокрапкове з'єднання. Крім того, кінцеві точки повинні підтверджувати прийняття кожного повідомлення. Протокол AMQP забезпечує асинхронну передачу даних, на базі моделі видавець/підписник.Даний стандарт описує також опціональний режим транзакцій з формально багатофазною послідовністю відновлення транзакцій. Залишаючись вірним своїм походженням в банківській галузі, проміжне

програмне забезпечення AMQP сфокусовано на спостереженні за всіма повідомленнями і забезпеченні їх доставки за призначенням, незалежно від наявності збоїв і перезавантаження системи.

AMQP використовується головним чином в обміні діловими повідомленнями. Зазвичай під «пристроями» розуміють мобільні телефони, що підтримують зв'язок з центрами обробки даних в операційних офісах. У разі «Інтернету речей» AMQP найкращим чином підходить для реалізації функцій «підсистеми управління» (control plane) або аналітичних функцій на базі серверів.

Головною перевагою цього протоколу є функція збереження та пересилання, яка забезпечує надійність, навіт після збою в мережі.

Протокол CoAP. CoAP **(**Constrained Application Protocol) – обмежений потокол передачі даних, призначений для передачі даних по лініям з обмеженою пропускною здатністю [20]. Цей протокол є аналогічним HTTP, але адаптований для роботи з "розумними" пристроями низької продуктивності. Так, на відміну від протоколу HTTP, який є текстовим і використовує TCP, CoAP – це бінарний протокол, який транспортується через UDP, що призводить до зменшення розміру його службових даних та збільшує гнучкість в моделях зв'язку.

CoAP організований у два шари: Шар транзакцій і шар «Request / Response».

Шар транзакцій обробляє єдиний обмін повідомленнями між кінцевими точками. Повідомлення обміну на цьому шарі можуть бути чотирьох типів:

- «Confirmable» - вимагає підтвердження;
- «Non-confirmable» - не вимагає підтвердження;
- квитирование - підтверджує отримання «Confirmable» повідомлення;
- «Reset» - вказує на те, що «Confirmable» повідомлення було отримано, але контекст, що підлягає обробці, відсутня.

Даними повідомленнями CoAP забезпечує механізм власної надійності [20].

Шар «Request / Response» Представляє модель взаємодії «запит / відповідь» (клієнт / сервер) для маніпулювання ресурсами і передачі. Сенсорний вузол зазвичай є сервером, але може реалізовувати обидва стилю спілкування, що скорочує час розробки та ресурси, необхідні на пристроях. У CoAP підтримується шифрування, але без TCP стандартний TLS не може бути використаний для забезпечення безпеки зв'язку. Тому в CoAP використовується DTLS (Datagram Transport Layer Security), новіша похідна TLS, яка за рахунок доповнень дозволяє йому працювати на вершині свого UDP транспортного протоколу.

Кожен з цих протоколів широко поширений. Є принаймні 10 варіантів реалізації кожного з них. Сучасний Інтернет підтримує сотні протоколів. «Інтернет речей» буде підтримувати ще на сотні протоколів більше. Важливо усвідомити сферу застосування кожного з них. Тому в табл. 2 зведено порівняльну характеристику деяких із цих протоколів.

Таблиця 2. Порівняння найпоширеніших протоколів прикладного рівня

Протокол	CoAP	AMQP	XMPP	MQTT
Опис протоколу	Для мережі з обмеженими ресурсами, низьким енергоспоживанням. Враховує різні питання реалізації в обмежених мережах	Система організації черг для з'єднання серверів між собою (S2S)	Протокол для з'єднання пристроїв з людьми, приватний випадок D2S – схема, коли люди з'єднуються з серверами.	Протокол для збору даних з пристроїв і передачі їх до серверів. (D2S)
Безпека	DTLS	TLS/SSL	TLS/SSL	TLS/SSL
Транспортний рівень	UDP	TCP	TCP	TCP
Якість обслуговування	+	+	-	+
Архітектура	Запит/відповідь	Видавець/ підписник	Видавець/підписник Запит/відповідь	Видавець/ підписник

Висновки

Таким чином, проаналізувавши основні протоколи IoT, було визначено що для «Інтернету речей» потрібно безліч протоколів. Всі протоколи, які були розглянуті в даній статті, помітно різняться між собою. Ймовірно, простіше за все класифікувати їх за кількома ключовими параметрами: якістю сервісу, адресацією і за додатком протоколів. Мабуть, ключові особливості протоколів залежать і від їх передбачуваного застосування. Наприклад, включення освітлення (в цьому випадку оптимальним варіантом є XMPP) абсолютно відрізняється від моніторингу ліній передачі (MQTT) або аналізу споживання енергії в центрі обробки даних (AMQP). Для MQTT і CoAP характерні менші накладні витрати на передачу даних (у зв'язку з невеликою кількістю службового трафіку) і меншою смугою пропускання.

Також було проведено порівняння основних безпроводових технологій для концепції Інтернету Речей. Основні завдання технологій – різні, різні архітектури та можливості. Тому, до вибору оптимальної технології для свого застосування потрібно підходити грунтовно, і об'єктивно, зважувати всі переваги та недоліки кожної з них.

Список літератури

1. Марек Б.А., Корченко О.Г., Карпінський М.П., Одарченко Р.С. Дослідження вразливостей сенсорних підмереж архітектури Інтернету речей до різних типів атак // Безпека інформації. - Т. 22, № 1 (2016). С. 12-19.

2. Корченко О.Г., Марек Богуслав Алєксандер, Одарченко Р.С., Абду Ахмад Алі Наджі, Петренко О.Ю. Аналіз загроз та механізмів забезпечення інформаційної безпеки в сенсорних мережах // Захист інформації, Т. 18, №1, січень-березень 2016. – С. 48-56

3. Интернет вещей: учебное пособие // А.В.Росляков, С.В.Ваняшин, А.Ю.Гребешков. – Самара: ПГУТИ, 2015. – 200 с.

4. Яка мережа «зловить» речі? – [Електронний ресурс]– електронні текстові дані – Режим доступу: http://mikrotik.kpi.ua/index.php/courses-list/iot/104-what-network-catch-things

5. Understanding IoT Protocols – Matching your Requirements to the Right Option. – [Електронний ресурс] – електронні текстові дані – Режим доступу: https://solace.com/blog/use-cases/understanding-iot-protocols-matching-requirements-right-option?utm_source=adroll&utm_medium=cpc&utm_campaign=iot&utm_content=25

6. Recommendation Y.2060 – [Електронний ресурс] – електронні текстові дані – Режим доступу: https://www.itu.int/rec/T-REC-Y.2060-201206-I

7. R. Odarchenko, A. Abakumova; O. Tkalich; O. Ustinov. LTE and wireless sensor networks integration in the concept of "Smart Home" // 2016 4th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC) pp. 35-38.

8. Одарченко Р.С., Гнатюк С.О., Ткаліч О.П. Архітектура сучасної захищеної інформаційно-комунікаційної мережі аеропорту // Захист інформації. – 3 (17). – С. 240-246.

9. Технологія Bluetooth Protocols – [Електронний ресурс] – електронні текстові дані – Режим доступу: http://wiki.kspu.kr.ua/index.php/Технологія_Bluetooth

10. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання. – Видання 2. – За загальною ред. Довгого С.О. – К.: «Азимут-Україна». – 2013. – 608с.

11. Как выбрать стандарт связи для сети IoT– [Електронний ресурс] – електронні текстові дані – Режим доступу: http://savepearlharbor.com/?m=201602&paged=59

12. Fahier N., Fang W.-C. An Advanced Plug-and-Play Network Architecture for Wireless Body Area Network Using HBC, ZigBee and NFC // IEEE International Conference on Consumer Electronics (ICCE). 2014. pp. 165–166.

13. Киричек Р. В., Парамонов А. И., Прокопьев А. В., Кучерявый А. Е. Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. № 4 (8). С. 29–41. URL: http://www.sut.ru/doci/nauka/review/4-14.pdf

14. Одарченко Р.С. Концепція сенсорної мережі збору метеорологічних даних для системи регулювання випромінюваної потужності радіопередавальних пристроїв стільникових мереж // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем // Вип. 8. – 2013. – С. 53-61

15. Архитектура LoRaWAN сетей. – [Електронний ресурс] – електронні текстові дані – Режим доступу: http://lorawan.lace.io/lorawan-networks/

16. Раскрываем тайны 6LoWPAN//Новости электроники – №11 – 2015. – С.30-36.

17. Что такое LoRa? – [Електронний ресурс]– електронні текстові дані – Режим доступу: http://lorawan.lace.io/faqs/lora/

18. И.А.Гепко, В.Ф.Олейник, Ю.Д.Чайка, А.В.Бондаренко. Современные беспроводные сети: состояние и перспективы развития / учебное пособие – Киев, 2009 – 672 с.

19. Understanding The Protocols Behind The Internet Of Things– [Електронний ресурс] – електронні текстові дані – Режим доступу: http://www.electronicdesign.com/iot/understanding-protocols-behind-internet-things

20. AMQP Advanced Message Queuing Protocol. Protocol Specification– [Електронний ресурс] – електронні текстові дані – Режим доступу: https://www.rabbitmq.com/resources/specs/amqp0-8.pdf

21. MQTT, CoAP, IoT Protocols – [Електронний ресурс] – електронні текстові дані – Режим доступу: https://eclipse.org/community/eclipse_newsletter/2014/february/article2.php

22. IoT - современные телекоммуникационные технологии – [Електронний ресурс]– електронні текстові дані – Режим доступу: http://www.lessons-tva.info/articles/net/013.html

Статтю подано до редакції 21.08.2017