

УДК 004.75

Гіоргізова-Гай В.Ш.Національний технічний університет України
«Київський політехнічний Інститут імені Ігоря Сікорського»**Шеренковський А.О.**Національний технічний університет України
«Київський політехнічний Інститут імені Ігоря Сікорського»**ШЛЮЗ У СИСТЕМІ ІНТЕРНЕТУ РЕЧЕЙ**

У статті на основі аналізу еталонних моделей від найбільш впливових організацій, які займаються стандартизацією архітектури Інтернету речей (англ. Internet of Things, IoT), і пропозицій від лідерів ринку IoT виділено перелік основних функцій і характеристик шлюзів IoT і запропоновано критерії їх класифікації та порівняння. Запропоновані критерії покликані допомогти розробникам IoT-систем вибирати шлюзи необхідної функціональності й технічних характеристик за пропозиціями численних постачальників.

Ключові слова: шлюзи IoT, Інтернет речей, моделі архітектури IoT, критерії порівняння, туманні обчислення.

Постановка проблеми. Ринок Інтернету речей розглядається аналітиками як найбільш перспективний у найближчому десятилітті. Прогнозований загальний економічний ефект IoT вимірюється трильйонами доларів США [1]. Тому сьогодні велика кількість виробників пропонує компоненти для IoT рішень, серед яких важливе місце посідають шлюзи. При цьому функції шлюзів і їх призначення в різних IoT проектах суттєво відрізняються.

Загалом шлюзи IoT являють собою мережеве обладнання, яке знаходиться на кордоні між ОТ (англ. Operational Technology) – апаратно-програмними комплексами для контролю й управління фізичними процесами, та ІТ (англ. Information Technology) – системами й мережами для створення, обробки, зберігання, забезпечення безпеки й обміну будь-якими формами електронних даних. Але, на відміну від більш звичних для ОТ та ІТ компонентів (датчики, контролери, модеми, маршрутизатори, протоколи каналів зв'язку, IoT-платформи), аналітичні огляди для шлюзів практично відсутні.

Аналіз останніх досліджень і публікацій. Зараз стандартизацією архітектури IoT займається багато організацій. Серед найбільш впливових можна виділити такі:

Міжнародний союз електрозв'язку – сектор стандартизації в галузі телекомунікацій (англ. International Telecommunication Union – Telecommunication Standardization Sector, ITU-T).

Всесвітній форум IoT (англ. IoT World Forum, IWF) – щорічна міжнародна конференція з Інтер-

нету речей, що спонсорується галуззю та об'єднує представників бізнесу, державних структур, провідних академічних закладів і провідних експертів галузі, таких як IBM, Intel, Cisco, Samsung тощо з метою просування IoT на ринок.

Національний інститут стандартів і технологій США (англ. The National Institute of Standards and Technology, NIST).

Консорціум індустріального Інтернету (англ. Industrial Internet Consortium, ІІС) – некомерційна група з відкритим членством, організована компаніями AT&T, Cisco, General Electric, IBM та Intel, що прагне усунути бар'єри між різними технологіями, забезпечити максимальний доступ до великих даних і вдосконалити інтеграцію фізичного й цифрового середовища.

Еталонна модель IoT від ITU-T. Еталонна модель IoT від Міжнародного союзу електрозв'язку (ITU-T) описана в Рекомендації Y.2060 [6, с. 6]. На відміну від більшості інших еталонних та архітектурних моделей, описаних у літературі, модель ITU-T деталізує фактичні фізичні компоненти екосистеми IoT, зосереджуючи увагу на тих елементах екосистеми IoT, які повинні бути з'єднані, інтегровані, керовані та надані додаткам. Детальна специфікація екосистеми описує вимоги до можливостей IoT.

На рис. 1 зображена еталонна модель IoT від ITU-T, що складається з чотирьох рівнів плюс можливість управління й безпеки, які діють між рівнями.

Рівень додатку складається з усіх додатків, що взаємодіють з IoT-пристроями.



Рис. 1. Еталона модель IoT за рекомендацією Y.2060

Рівень підтримки послуг і підтримки додатків дає можливості, які використовуються додатками. До прикладів належить спільне опрацювання даних та управління БД.

Рівень мережі виконує дві базові функції. Можливості мережі належать до взаємодії пристроїв і шлюзів. Транспортні можливості належать до транспорту інформації служб і додатків IoT, а також інформації управління й контролю IoT.

Рівень пристроїв включає в себе різноманітні пристрої, оснащені датчиками, і підтримує широкий спектр бездротових і дротових технологій передачі даних і мережевих протоколів. Можливості обробки даних у таких пристроїв, як правило, обмежені. До цього ж рівня належать і шлюзи, які з'єднують пристрої з мережами зв'язку. Шлюзи виконують необхідну трансляцію між протоколами, що використовуються в мережах зв'язку і пристроях.

Рівень можливостей управління охоплює функції управління пристроями та мережею, тобто управління несправностями, управління конфігурацією, управління обліком, управління показниками роботи й управління безпекою.

Рівень можливостей безпеки включає загальні можливості забезпечення безпеки, які не залежать від додатків.

За рекомендацією Y.2060 пристрої можуть спілкуватись між собою декількома шляхами.

Перша можливість – зв'язок між пристроями через шлюз. Наприклад, за допомогою шлюзу пристрій із підтримкою Bluetooth може здійснювати зв'язок із пристроєм збирання даних або пристроєм загального призначення, що використовують Wi-Fi. Друга можливість – зв'язок по мережі зв'язку без шлюзу. Наприклад, якщо всі пристрої підтримують Bluetooth, вони можуть управлятися з комп'ютера, планшета або смартфона з підтримкою Bluetooth. Третя можливість – прямий зв'язок пристроїв між собою через окрему локальну мережу, тоді як зв'язок із зовнішньою мережею здійснюється через шлюз LAN.

Рекомендація Y.2067 [7, с. 5] закріплює вимоги до шлюзів IoT, які зазвичай розпадаються на три категорії:

Шлюз підтримує різні технології доступу до пристроїв, даючи пристроям змогу обмінюватися даними один із одним і з мережею Інтернет або корпоративною мережею, що містить додатки IoT. Такі схеми доступу можуть, наприклад, включати ZigBee, Bluetooth і Wi-Fi тощо.

Шлюз підтримує необхідні мережеві технології як для локальних, так і для глобальних мереж. Ці технології можуть включати в себе Ethernet і Wi-Fi на території організації, а також стільниковий зв'язок, Ethernet, xDSL і кабельний доступ до Інтернету і глобальних корпоративних мереж.

Шлюз підтримує взаємодію з додатками, управління мережею й функції безпеки.



Рис. 2. Еталонна модель Всесвітнього форуму IoT

Дві перші вимоги включають у себе трансляцію протоколів між різними мережевими технологіями і стеками протоколів. Третя вимога зазвичай називається функцією IoT-агента. По суті, IoT-агент надає функціональність високого рівня від імені IoT-пристроїв, таку як організація або резюмування даних із декількох пристроїв для передачі в IoT-додатки, забезпечення протоколів і функцій безпеки та взаємодія із системами управління мережею.

Еталонна модель Всесвітнього форуму IoT. Комітет з архітектури Всесвітнього форуму IoT, що складається з лідерів індустрії, включаючи IBM, Intel та Cisco, в жовтні 2014 року опублікував еталонну модель IoT. Ця еталонна модель є корисним доповненням до моделі ITU-T. Якщо документи ITU-T основну увагу приділяють рівням пристрою та шлюзу й описують верхні рівні лише в загальних рисах, то IWF стурбований більш масштабним питанням розроблення додатків, проміжного програмного забезпечення й функцій підтримки для корпоративного Інтернету речей.

IWF вважає еталонну модель IoT прийнятною в галузі базовою структурою, спрямованою на стандартизацію концепцій і термінології, визначення необхідного функціоналу та проблем, які потребують вирішення до того, як галузь зможе реалізувати цінність IoT.

Запропонована семирівнева модель IWF зображена на рис. 2 й добре описана у праці [8].

Рівень 1 утворюють фізичні пристрої та контролери, які можуть керувати кількома пристроями. Рівень 1 моделі IWF приблизно відповідає рівню пристрою в моделі ITU-T (рис. 1).

Рівень 2 моделі IWF приблизно відповідає рівню мережі в моделі ITU-T. Основна відмін-

ність у тому, що модель IWF зараховує шлюзи до рівня 2, тоді як у моделі ITU-T вони належать до рівня 1. Оскільки шлюз є мережевим пристроєм і пристроєм зв'язку, зарахування його до рівня 2 виглядає більш логічним.

З логічного погляду цей рівень реалізує зв'язок пристроїв між собою та між пристроями й низькорівневою обробкою на рівні 3. З фізичного погляду цей рівень складається з мережевих пристроїв, таких як маршрутизатори, комутатори, шлюзи і брандмауери, що використовуються для створення локальних і глобальних мереж і підключення до Інтернету. Цей рівень дає пристроям змогу здійснювати зв'язок один із одним і за допомогою більш високих логічних рівнів обмінюватися даними з прикладними платформами, такими як комп'ютери, пристрої дистанційного управління і смартфони.

Рівень 3 описує первинну обробку даних на рівні периферійних обчислень, які іноді називається туманними обчисленнями (Fog Computing) [2]. Туманні обчислення й туманні служби, як очікується, стануть відмінною характеристикою IoT. Туманні обчислення представляють у сучасних мережевих технологіях тренд, протилежний хмарним обчисленням. У туманних обчисленнях велике число окремих інтелектуальних об'єктів здійснює зв'язок із туманними мережевими структурами, які здійснюють обчислення і зберігають ресурси поряд із периферійними пристроями в IoT. Туманні обчислення вирішують проблеми, що виникли внаслідок діяльності тисяч або мільйонів «розумних» пристроїв, включаючи проблеми безпеки, конфіденційності, обмежених можливостей мережі й затримки. Термін «туманні обчислення» обраний тому, що туман стелиться по землі, тоді як хмари знаходяться високо в небі.

Рівень 4 – рівень накопичення даних. Дані, що надійшли з різних пристроїв, профільтовані й оброблені рівнем периферійних обчислень, поміщаються в сховище, де будуть доступні для більш високих рівнів. Ще один погляд на рівень накопичення даних полягає в тому, що він є кордоном між інформаційними технологіями (ІТ) та операційними технологіями (ОТ).

Рівень 5 займається перетворенням накопичених даних. Основними операціями, що виконуються на цьому рівні, є такі:

- перетворення «даних у русі» в «дані у спокої»;
 - перетворення формату з мережевих пакетів у реляційні таблиці БД;
 - перехід від обчислень за подіями до обчислень за запитом;
- значне зниження обсягу даних за рахунок фільтрації й вибіркового зберігання.

Рівень 6 містить додатки будь-якого типу, що використовують дані IoT на вході або керують IoT-пристроями. Як правило, додатки взаємодіють із рівнем 5 і з «даними у спокої», тому їм не обов'язково функціонувати на швидкостях мережі.

Рівень 7 з'явився в результаті визнання того факту, що IoT буде корисний лише тоді, коли з ним зможуть взаємодіяти люди. Цей рівень може включати кілька додатків та обмін даними й/або керуючою інформацією по Інтернету чи корпоративній мережі.

Треба підкреслити, що модель передбачає також спрощений режим роботи системи IoT, який дає можливість додаткам оминати проміжні рівні й безпосередньо взаємодіяти з рівнем 3 або навіть із рівнем 2. У такому випадку логічно дати шлюзам можливість здійснювати також і функції периферійних/туманних обчислень. Компанія Cisco, яка бере активну участь в IWF, явно позиціонує свої шлюзи як пристрої, що проводять аналітику даних і реагують на події.

Еталонні моделі NIST та ІІС. Якщо МСЕ-Т і IWF намагаються надати всеохоплюючі моделі IoT з урахуванням перспектив його розвитку, то моделі Національного інституту стандартів і технології США [3, с. 22; 4, с. 2] та консорціуму індустріального Інтернету [5, с. 38] можна розглядати як певне спрощення й деталізацію попередніх для конкретного застосування.

Модель ІІС для шлюзів виділяє функції аналітики краю, що по факту є додаванням до можливостей шлюзу рівня туманних обчислень із моделі IWF. У моделі NIST шлюз одразу називається агрегатором і належить до апаратного забезпечення, що займається дослідженням даних від

датчиків. Його визначають як певний сервер, що знаходиться в безпосередній близькості до речей.

Усі розглянуті еталонні моделі віддають шлюзу функції створення локальних мереж для підключення неінтелектуальних пристроїв та узгодження протоколів під час взаємодії між ОТ та ІТ. Мережа пристроїв може мати як стандартний TCP/IP стек протоколів і бути реалізована за допомогою Wi-Fi мережі або дротового підключення, так і бути не IP мережею та підключати датчики за допомогою таких технологій, як Bluetooth, ZigBee або 6LoWPAN тощо. Усі моделі, крім ІТУ, визначають для шлюзів функції безпеки й управління на рівні пристроїв і мережі, модель ІТУ – тільки на рівні пристроїв. Також усі організації зі стандартизації, окрім ІТУ, надають шлюзам ще й функції аналітики краю між ОТ та ІТ.

Аналіз пропозицій ринку IoT. Як можна побачити з огляду пропозицій [9–16], лідери ринку IoT Intel, Hewlett Packard, Cisco, Dell Technologies, а також компанії, які на цьому ринку недавно, – Huawei, NEXCOM, Monnit, Davra Networks тощо, підтримують увесь спектр перерахованих функцій. Усі з розглянутих виробників пропонують як універсальні шлюзи для використання в різних галузях промисловості, так і рішення для окремих вертикалей ринку. Лінійки шлюзів, що пропонуються, включають як малопотужні енергоефективні моделі для «легких» економних проєктів, наприклад, NEXCOM, молодші моделі Dell та Intel, так і промислові моделі, спрямовані на аналітику та зберігання великих об'ємів даних, найяскравішим представником останніх є конвергентні системи Hewlett Packard. Серйозні постачальники наділяють свої шлюзи ПЗ для інтеграції у власні (Eurotech, Davra Networks) або сторонні хмарні платформи, наділяють шлюзи власними платформами й ПЗ для захисту й управління пристроями та мережею (Hewlett Packard, Cisco, Dell, Huawei) або підтримують рішення від сторонніх компаній. Деякі виробники (Hewlett Packard, Cisco, Huawei) пропонують власні рішення для аналітики, обробки, зберігання й візуалізації великих обсягів даних, інші – забезпечують програмно-апаратні платформи для сторонніх рішень, що вже зарекомендували себе на ринку IoT.

Постановка завдання. Для спрощення вибору шлюзів від численних виробників під час проєктування IoT-систем необхідна систематизація їх функцій, формування критеріїв їх класифікації та порівняння.

Виклад основного матеріалу дослідження. Узагальнюючи аналіз еталонних моделей IoT, можна

виділити перелік наведених нижче функцій і характеристик шлюзів. Важливо підкреслити, що сьогодні більшість виробників особливо в старших моделях своїх шлюзів забезпечує можливості як первинної обробки даних, до якої зазвичай зараховують обробку подій і прийняття рішень у режимі реального часу, нормалізацію й фільтрацію даних для подальшої передачі на хмарний сервер, так і повноцінну аналітику зі зберіганням і візуалізацією даних.

1. Підтримка первинних і периферійних/туманних обчислень.

У якості критеріїв вибору варто звернути увагу на таке:

Підтримка шлюзом надійної спеціалізованої ОС (наприклад, від Wind River, Cisco, Microsoft).

Наявність у фірми розробника шлюзу готових додатків для обробки даних, якість і можливості цих додатків, а також можливість підтримки їх цією моделлю шлюзу.

Наявність у фірми розробника платформ для розроблення замовником власного додатку зі зручними інтерфейсами прикладного програмування (API) та комплектами розробки ПЗ.

Можливості вибору ОС, мов і засобів програмування для реалізації власного додатка забезпечують адаптацію до потреб проекту.

2. Підтримка необхідних технологій доступу до пристроїв для обміну даними між ними та з корпоративними або хмарними додатками IoT. Тут відображуються можливості збирання даних із різних джерел, їх інтеграції, уніфікації представлення протоколів і форматів даних. У цьому пункті варто звернути увагу на таке:

Максимальна кількість пристроїв, із якими може взаємодіяти шлюз.

Перелік інтерфейсів із пристроями, в який можуть входити як сучасні протоколи дротових і бездротових мереж (Ethernet, Wi-Fi, Zigbee, 6LoWPAN, Bluetooth Low Energy тощо), так й успадковані протоколи (BACNet, Modbus і CANbus тощо).

Перелік інтерфейсів із зовнішнім сервером додатків, у який можуть входити протоколи дротових і бездротових мереж: Ethernet, Wi-Fi, протоколи стільникового зв'язку тощо.

Підтримка GPS разом зі стільниковим зв'язком забезпечить ефективну роботи з мобільними об'єктами з географічною прив'язкою, наприклад, транспортом.

Наявність хорошого інтерфейсного профілю, заснованого на реалізації універсального самоналаштування (англ. Universal Plug and Play, UPnP), що визначає протокол для взаємодії з різними пристроями.

3. Функції маршрутизатора. Оскільки шлюз є вузлом стандартної IP мережі під час взаємодії із сервером обробки даних, то він зобов'язаний підтримувати мінімальні функції маршрутизатора. Водночас низка виробників (наприклад, Cisco, Intel, Huawei) позиціонує деякі моделі своїх шлюзів як повноцінні багатопортові маршрутизатори. У цьому випадку можна виділити такі можливості:

Підтримка маршрутизації між декількома провідними чи Wi-Fi локальними IoT мережами.

Підтримка поширених функцій IP маршрутизаторів – протоколів маршрутизації, DHCP, таблиць доступу, міжмережових екранів тощо.

4. Функції управління кінцевими пристроями мережею й додатками.

Управління пристроями включає можливості їх виявлення й аутентифікації, конфігурацію, діагностику, оновлення прошивки та/або ПЗ, управління робочим статусом пристрою.

Управління мережею включає можливості управління її моніторингом і конфігурацією, виявлення й керування перевантаженнями, керування трафіком, вимогами QoS.

Управління додатками включає можливості керування їх установленням і видаленням, виконанням оновлень, резервним копіюванням, відстеженням та усуненням несправностей.

5. Функції безпеки пристроїв, мережі й додатків. Як підкреслюється всіма без винятку авторами, ці функції для IoT є життєво важливими.

Захист на рівні ПЗ включає авторизацію, аутентифікацію, конфіденційність і цілісність даних програми, захист недоторканності приватного життя, аудит безпеки й антивірусний захист.

Захист на рівні мережі включає авторизацію, аутентифікацію, конфіденційність даних, конфіденційність і цілісність даних сигналізації.

Захист на рівні пристрою включає аутентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом, захист конфіденційності й цілісності даних.

Функції управління й безпеки всі крупні вендори забезпечують засобами власних платформ, власних ОС, таких як Wind River Linux, Windows 10 IoT, Cisco IOS, додатковими апаратними засобами (Dell, Cisco), власними пакетами ПЗ, а також підтримкою стандартних рішень і сертифікованих рішень від сторонніх компаній.

6. Інші характеристики.

У рамках подібної функціональності шлюзи можуть відрізнятися технічними характеристиками, серед яких можна виділити такі:

Обчислювальна потужність, об'єми пам'яті і її типи, що важливо врахувати під час планування реалізації на шлюзі додатків.

Форм фактор – компактність і форма конструктивного виконання, що важливо врахувати під час планування місця розташування шлюзу.

Умови експлуатації. Одні пристрої придатні лише для роботи у звичайних приміщеннях, інші – розраховані на роботу в широкому діапазоні температур, в умовах підвищеної вологості, запиленості.

Варто також звернути увагу на те, що ринок послуг і пристроїв IoT зазвичай поділяють на два великі сегменти: *промисловий* і *споживчий*, які відрізняються вимогами до ціни, надійності, безпеки, потужності, масштабованості. У цих рамках вендори можуть надавати як універсальні пристрої, так і пристрої для конкретних вертикалей ринку в складі комплексних рішень. Більшість виробників орієнтуються на промисловий ринок, хоча молодші моделі їхніх рішень, наприклад,

Intel, Dell, цілком підходять для простих економічних рішень, а продукція таких компаній, як Google чи Samsung, передусім орієнтована на споживчий ринок.

Висновки. Моделі архітектури IoT корисні як для постачальників, що розробляють функціональні елементи всередині моделі, так і для замовників, допомагаючи їм виробляти свої вимоги й оцінювати пропозиції постачальників. Розглянуті моделі визначають основні функції шлюзів і їх місце в екосистемі IoT.

Сьогодні на ринку IoT присутня велика кількість визнаних і менш відомих виробників, також щороку з'являються нові. Різні виробники пропонують як окремі моделі, так цілі модельні ряди шлюзів, які загалом охоплюють увесь спектр перерахованих функцій. Тому гадаємо, що запропоновані критерії класифікації та порівняння допоможуть розробникам IoT проектів вибирати шлюзи необхідної функціональності й технічних характеристик за пропозиціями різних постачальників.

Список літератури:

1. The Internet of Things: Mapping the Value Beyond the Hype. 2015. *Офіційний сайт McKinsey Global Institute*. URL: http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world (дата звернення: 17.06.2018).
2. Transformation to a Next Generation IoT. 2015. *Офіційний сайт міжнародного форуму IoT*. URL: <https://www.iotwf.com/resources/108> (дата звернення: 17.06.2018).
3. Voas J., Kuhn R. et al. Internet of Things (IoT) Trust Concerns. NIST Cybersecurity White Paper. October, 2018. URL: <https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/10/17/iot-trust-concerns/draft/documents/iot-trust-concerns-draft.pdf> (дата звернення: 17.06.2018).
4. Voas J. Networks of Things, NIST Special Publication (SP) 800-183, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2016. URL: <https://www.actiac.org/system/files/NIST%20SP%20800-183.pdf> (дата звернення: 17.06.2018).
5. The Industrial Internet of Things. 2017. *Офіційний сайт консорціуму індустріального Інтернету*. URL: http://www.iiconsortium.org/II_C_PUB_G1_V1.80_2017-01-31.pdf (дата звернення: 17.06.2018).
6. Recommendation Y.2060. Overview of the Internet of Things. ITU-T, Geneva. June 2012.
7. Recommendation Y.2067. Common Requirements and Capabilities of a Gateway for Internet of Things Applications. ITU-T, Geneva. June 2014.
8. Stallings W. The Internet of Things: Network and Security Architecture, The Internet Protocol Journal Vol. 18, No 4, Desember 2015.
9. Dell змінює економіку Інтернету речей з новими компактними шлюзами Edge Gateway. 2017. *Офіційний сайт компанії Dell*. URL: www.dell.com/learn/ua/ru/uacorp1/press-releases/dell-changing-economy-of-iot-with-new-compact-gateways-edge-gateway (дата звернення: 17.06.2018).
10. Короткий огляд апаратних платформ, типових архітектурних рішень і послуг для корпоративних інформаційних систем. 2018. *Офіційний сайт компанії Hewlett Packard*. URL: <https://h20195.www2.hp.com/v2/GetPDF.aspx/c04771945.pdf> (дата звернення: 17.06.2018).
11. Пятницких А. Облачные технологии в автоматизации: комплексный подход от Eurotech. *Control Engineering Россия*. 10.2016. С. 62. URL: <https://controlengrussia.com/internet-veshhej/eurotech/> (дата звернення: 17.06.2018).
12. Huawei AR Series Agile Gateways Brochures. 2017. *Офіційний сайт компанії Huawei*. URL: http://www.huawei.com/minisite/iot/img/hw_ar_series_agile_gateways_brochure_en.pdf (дата звернення: 17.06.2018).
13. О'Доннелл Л. 15 наиболее продвинутых производителей оборудования Интернета вещей. 2017. URL: <http://www.pcweek.ua/themes/detail.php?ID=155790> (дата звернення: 17.06.2018).

14. IoT Gateway. 2018. *Офіційний сайт компанії NEXCOM*. URL: <http://www.nexcom.com/Products/industrial-computing-solutions/iot-solutions/iot-gateway> (дата звернення: 17.06.2018).
15. Cisco IoT Networking. 2017. *Офіційний сайт компанії Cisco*. URL: <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/brochure-c02-734481.pdf> (дата звернення: 17.06.2018).
16. Технологія Intel IoT Gateways. 2018. *Офіційний сайт компанії Intel*. URL: <https://software.intel.com/ru-ru/iot/hardware/gateways> (дата звернення: 17.06.2018).

ШЛЮЗ В СИСТЕМЕ ІНТЕРНЕТА ВЕЩЕЙ

В статье на основе анализа эталонных моделей наиболее влиятельных организаций, которые занимаются стандартизацией архитектуры Интернета вещей (англ. Internet of Things, IoT), и предложений лидеров рынка IoT выделен перечень основных функций и характеристик шлюзов IoT, предложены критерии их классификации и сравнения. Критерии призваны помочь разработчикам IoT-систем выбрать шлюзы необходимой функциональности и технических характеристик из предложений многочисленных поставщиков.

Ключевые слова: шлюз IoT, Интернет вещей, модели архитектуры IoT, критерии сравнения, туманные вычисления.

GATEWAY IN THE INTERNET OF THINGS SYSTEM

In the article, based on the analysis of reference models of the most influential organizations that are engaged in standardization of the architecture of the Internet of Things (IoT), and offers from IoT market leaders, a list of the main functions and characteristics of IoT gateways is highlighted, and criteria for their classification and comparison are proposed. The criteria are designed to help IoT system developers choose the gateways of the required functionality and technical characteristics from the offers of numerous vendors.

Key words: IoT gateway, Internet of things, IoT architecture models, comparison criteria, fog computing.