УДК 621.395.348.4 DOI: 10.31673/2412-4338.2019.041227

Сорокін Д. В., Бондарчук А.П., Сторчак К.П.
Державний університет телекомунікацій, Київ

ІНФРАСТРУКТУРА ПРОМИСЛОВИХ МЕРЕЖ IOT ТА КІБЕРЗАГРОЗИ В ДОСТУПІ ПРИ ВИКОРИСТАННІ IOT РІШЕНЬ

Поява в Україні операторських мереж з концепцією доступу IoT потребує розробки технічних та програмних засобів для управління відповідними пристроями та сервісами. Найбільша кількість кейсів спостерігається в обслуговуванні приватних виробничих мереж M2M, державних мереж з обмеженим або закритим доступом, приватних домашніх мереж, в тому числі, приватних комунальних господарств,.

Розглянуто особливості побудови IoT мереж в цілому, визначено їх завдання та специфіку фізичної архітектури IoT рішень. Проведено аналіз процесів формування, перетворення та передачі фізичних сигналів в мережі IoT. Визначено, що підсистеми IoT стикуються ненадійним каналом зв'язку, тому потребують розробки механізмів гарантованої доставки інформації.

Проведено аналіз інфраструктури рішень IoT, що використовуються в промисловості для автоматизації промислових сервісів. Розглянуто структурну схему розгортання інфраструктури LPWAN мережі. Наведено перелік конкурентних платформ, що можуть використовуватися для автоматизації промислових сервісів.

Підняте питання кібербезпеки в мережах IoT. Проведено аналіз інцидентів несанкціонованих втручання в мережу, які призвели до тимчасової відмови сервісів та заподіяли значної шкоди кінцевим споживачам послуг. Розглянуто методи перешкоджання кібератакам в мережах IoT.

Проведено аналіз використання рішень на основі стандарту NB-IoT та рішень на базі IoT для автоматизації промислових сервісів та з точки зору забезпечення безпеки в приватних мережах. Запропоновано методику вибору рішення з урахуванням вимог до бізнес-процесів кінцевих споживачів сервісів та технічних можливостей оператора. Розглянуто переваги приватних NB-IoT-мереж порівняно з LPWAN.

Ключові слова: *технології LPWAN, мережа IoT, приватні IoT мережі, інфраструктура рішень IoT, промислові сервіси, кібербезпека в мережах IoT, стандарт NB-IoT.*

Sorokin D. V., Bondarchuk A.P., Storchak K.P.
State University of Telecommunications, Kyiv

INDUSTRIAL NETWORK INFRASTRUCTURE IoT & CYBERSECURITY IN USE IoT SOLUTIONS

The emergence of operator networks with the concept of IoT access in Ukraine requires the development of hardware and software to manage the respective devices and services. The largest number of cases is observed in the services of private M2M production networks, public networks with restricted or closed access, private home networks, including private utilities,.

The features of building IoT networks in general are considered, their tasks and specifics of physical architecture of IoT solutions are defined. The processes of formation, transformation and transmission of physical signals in the IoT network are analyzed. It is determined that IoT subsystems are interconnected by an unreliable communication channel and therefore require the development of mechanisms of guaranteed delivery of information.

The infrastructure of IoT solutions used in industry for automation of industrial services is analyzed. The structural scheme of deployment of LPWAN network infrastructure is considered. The list of competing platforms that can be used for automation of industrial services is given.

Raised the issue of cybersecurity on IoT networks. The analysis of incidents of unauthorized network interventions that led to temporary denial of services and caused significant damage to end users of services.

Methods of preventing cyberattacks in IoT networks are considered.

The analysis of the use of NB-IoT and IoT solutions for automation of industrial services and security in private networks is analyzed. The method of choice of the decision in view of requirements to business processes of end users of services and technical capabilities of the operator is offered. The advantages of private NB-IoT networks over LPWAN are considered.

***Keywords**: LPWAN technologies, IoT network, private IoT networks, IoT solution infrastructure, industrial services, cyber security in IoT networks, NB-IoT standard.*

Сорокин Д. В., Бондарчук А.П., Сторчак К.П.

Государственный университет телекоммуникаций, Киев

ИНФРАСТРУКТУРА ПРОМЫШЛЕННЫХ СЕТЕЙ IoT, А ТАК ЖЕ КИБЕРУГРОЗЫ В ДОСТУПЕ IoT РЕШЕНИЯХ

Появление в Украине операторских сетей с концепцией доступа IoT требует разработки технических и программных средств для управления соответствующими устройствами и сервисами. Наибольшее количество кейсов наблюдается в обслуживании частных производственных сетей M2M, государственных сетей с ограниченным или закрытым доступом, частных домашних сетей, в том числе, частных коммунальных хозяйств,.

Рассмотрены особенности построения IoT сетей в целом, определены их задачи и специфика физической архитектуры IoT решений. Проведен анализ процессов формирования, преобразования и передачи физических сигналов в сети IoT. Определено, что подсистемы IoT стыкуются ненадежным каналом связи, поэтому нуждаются в разработке механизмов гарантированной доставки информации.

Проведен анализ инфраструктуры решений IoT, используемых в промышленности для автоматизации сервисов. Рассмотрена структурная схема развертывания инфраструктуры LPWAN сети. Приведен перечень конкурентных платформ, которые могут использоваться для автоматизации сервисов.

Поднят вопрос кибербезопасности в сетях IoT. Проведен анализ инцидентов несанкционированных вмешательств в сеть, которые привели к временному отказу сервисов и причинили значительный ущерб конечным потребителям услуг. Рассмотрены методы предотвращения кибератак в сетях IoT.

Проведен анализ использования решений на основе стандарта NB-IoT и решений на базе IoT для автоматизации сервисов и с точки зрения обеспечения безопасности в частных сетях. Предложена методика выбора решения с учетом требований к бизнес-процессам конечных потребителей сервисов и технических возможностей оператора. Рассмотрены преимущества частных NB-IoT-сетей по сравнению с LPWAN.

***Ключевые слова:** технологии LPWAN, сеть IoT, частные IoT сети, инфраструктура решений IoT, промышленные сервисы, кибербезопасность в сетях IoT, стандарт NB-IoT.*

Вступ.

Перспективи розвитку інтернет речей в світі вже очевидні. Приблизні показники на 2023 рік вказують, що понад 3,5 мільярдів пристроїв будуть підключені до IoT-мереж, з яких третина включень – це приватні мережі [8].

Сьогодні на телекомунікаційному ринку з’явилися IoT-компанії, що пропонують імплементувати різні кейси по впровадженню таких рішень. З'явилося безліч різних виробників обладнання, які впроваджують IoT мережі. Зокрема в поточному році в Україні з'явилися операторські мережі з концепцією доступу IoT.

Мережі IoT–рішень активно впроваджуються в повсякденне життя людини, активно впливають в розвитку і модернізації промислових організацій, державних установ, а також у всіх приватних мережах. Одночасно з розвитком IoT мереж, активно ведеться робота з розробки програмного забезпечення, для управління різними сервісами, пристроями – це дозволить проводити активну державну політику діджиталізації.

У перспективі, в найближчих два роки, будуть затребувані такі кейси рішень IoT, а саме:

I. Приватні домашні мережі, які можуть забезпечувати сервіси безпеки, економію витрат пов'язаних з комунальним господарством (енергозбереження, водопостачання), домашньої аналітикою (як крок до розвитку автоматизації домашньої мережі «Smart Home»), або модернізацію і розвиток приватних комунальних господарств («Smart City»);

II. Приватні виробничі мережі M2M (міжмашинна взаємодія «Machine-to-Machine»), зосереджені на сервісах промислової необхідності, телеметрія, автоматизації процесу виробництва, контроль бізнес-процесів, контроль якості та безпеки виконання робіт (перед усім в таких галузях економіки: як вугільна, енергетичної, гірничо-добувна, газова);

III. Державні мережі з обмеженим, або закритим доступом, послуги яких зосереджені на безпеки, фіксації та попередженні правопорушень, або застосуванням різних сценаріїв віддаленого управління об'єктами;

Основна частина.

IoT мережа – це система фізичних елементів, які підтримують фізичне з'єднання і взаємодіють за допомогою різних фізичних технологій для передачі інформації. Віддалені фізичні елементи мережі-IoT, з'єднуються по принципу останньої милі для кінцевого пристрою, який інтегрується в центр управління IoT–мережі. Основним завдання IoT-мережі є ідентифікація пристрою, вимірювання або відправка повідомлення про зміну даних, а також передача та обробка даних. Принципом концепції Інтернет речей є виконання всіх операцій в режимі максимально наближеного до реального часу. Автоматична обробка вхідних і вихідних даних, від переданих IoT-пристроїв, гарантує актуальність усіх даних в системі.

Доступ до віддалених сегментів мережі IoT–пристроїв здійснюється по радіодоступу. Радіо-IoT-пристрої характеризуються такими параметрами як дальність, швидкість та енергоефективність. Причому одночасно можна відповідати лише 2-м параметрам з 3-х.

Фізична архітектура IoT-рішень, умовно поділяється на два типи, або дві підсистеми, які включають в себе:

1. Велика кількість периферійних пристроїв з малими обчислювальними потужностями, низьким енергоспоживанням, високою швидкістю реакції на події – це рішення на впровадження (Embedded solutions) [5];
2. Хмарні сервера з високою обчислювальною потужністю для обробки великого масиву даних, їх зберігання та класифікація можливо з елементами машинного інтелекту і аналітики – це хмарні рішення (Cloud solutions) [5];.

В результаті інтеграції і синергії виходять комплексні рішення IoT.

До системи рішень на впровадження (Embedded solutions) відносяться датчики, які діляться на:

а) активні – випромінюють самі сигнали і приймають відображення;

б) пасивні – працюють тільки на прийом;

Пасивні датчики мають перевагу перед активними, за параметрами енергоспоживання. Більшість датчиків засноване на прийомі хвиль – звукових, ультразвукових, світлових різного діапазону, теплових. Однак є категорія датчиків, заснованих на зміні їх фізичних характеристик, таких як індуктивність, ємність, тиск. Гарні результати виходять від комбінації декількох датчиків, наприклад PIR детектор і ємнісний датчик для визначення руху.

Всі датчики формують аналоговий сигнал, який необхідно перевести в цифру для подальшої обробки, чим і займається A2D перетворювач. Після перетворення в цифровий формат, інформація з датчика повинна бути оброблена локальним процесором пристрою, так званим «хабом» (HUB). Головне його завдання проставити тег (Tag) отриманої інформації, для подальшої класифікації сигналу та ідентифікації. Теги (Tag) можуть бути простим, як наприклад – передача руху, так і складними – рух з даними про швидкість. Іноді потрібні багатовимірні теги (обсяг даних) [5]. Чим складніший тег, тим більше навантаження на процесор, в результаті збільшується енергоспоживання пристрою – датчика. З іншого боку, чим більше інформативний тег, тим менше необхідно кількість інформації, що передається в

«Cloud» і відповідно потрібна менше смуга пропускання, що в результаті призводить до збільшення швидкість реакції на подію. Всі теги мають часову мітку, для відображення оновлення даних за часовий період.

Після обробки отриманих сигналів так званим «хабом», отримані дані агрегуються на сервері, або в «Cloud». Агрегація даних відбувається за сценарієм фільтрації інформація, від різних датчиків і пристроїв підсумовується по однотипним тегам. При цьому самі типи пристроїв, які моделюють дані (датчики), можуть бути різні.

Зібрана інформація від всіх об'єктів, що підсумовують теги, систематизується аналітичним блоком. В аналітичний блок закладена основна логіка, або основний алгоритм системи. В результаті роботи основного алгоритму системи (аналітичний блоку системи – прикладний рівень), виводиться і передається в блок презентації для візуалізації користувачеві. Це може виглядати, як відправка повідомлення на мобільний пристрій, графік на WEB інтерфейс, або інші варіанти візуалізації і нотифікації [1]. На рис.1 наведена загальна архітектура IoT-рішення.

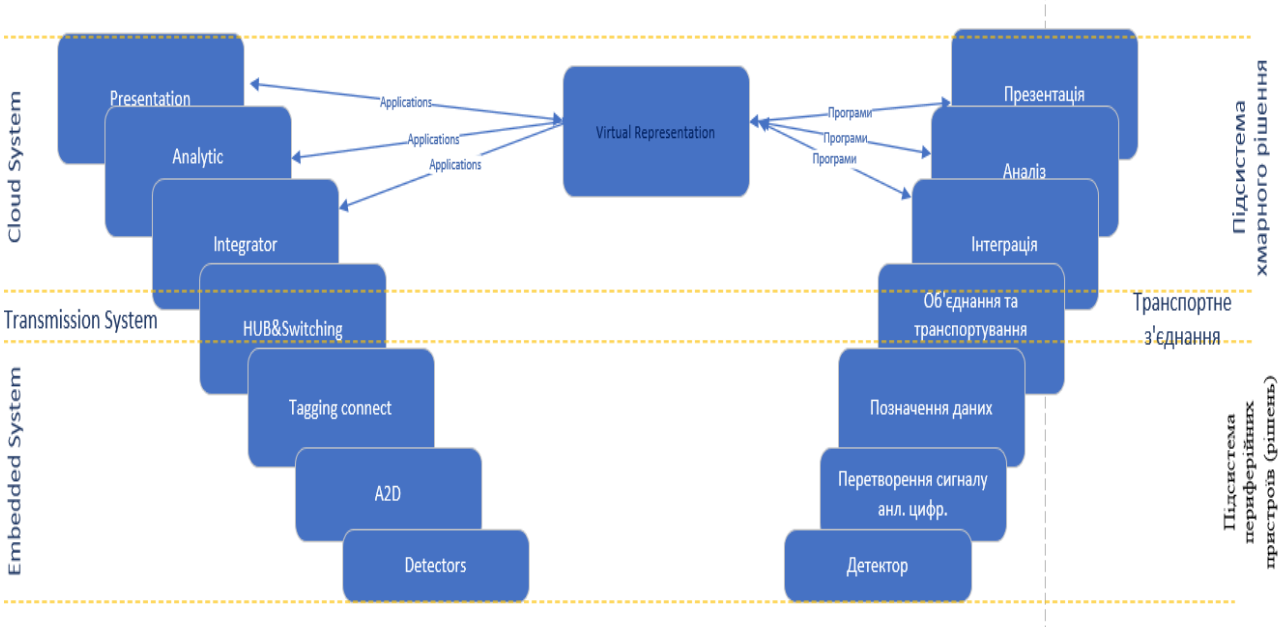

Рис.1. Загальна архітектура IoT-рішення

Умовно розділені підсистеми IoT стикуються ненадійним каналом зв'язку, тому доводиться мати механізми гарантованої доставки інформації. У випадку, якщо не вдається передати інформацію від «Хаба» (пристрій що відповідає за певний сегмент підконтрольних йому датчиками) в «Cloud», або на сервер, здійснюються повторні спроби передачі. Така схема має працювати і в іншу сторону. В таких випадках передбачений блок «Віртуального уявлення» периферійного пристрою, в який записується інформація для передачі периферійних пристроїв. Зміни в блок «Віртуального уявлення» можуть бути ініційовані з різних модулів вхідного ланцюга.

Можливе виникнення ситуації, при якій – теги з інформацією про аварії не були передані по причини ненадійного каналу зв'язку. Після певного проміжку часу з'явиться новий тег, про зміну роботи датчика (приклад: зміна відправленої інформації датчиками, які реєструють зміну навколишнього середовища, або параметрів у часі). Для уникнути цієї ситуації дуже важливо мати резервний канал зв'язку на «Хаб» пристрої, що дозволить виконати відправку усіх зареєстрованих повідомлень та змін подій, що відбуваються на датчиках.

Розробка алгоритму аналітичних IoT–програм починається зі списку подій, які можуть статися. Підсумовування тегів проводиться по групі периферійних пристроїв з однотипними тегами.

Модуль інтегрування, призначений для винесення рішення по апроксимації (передбачення

подальших дій), або детермінованість (виявлена ситуації з безліч варіантів). Ця інформація служить, для збудження модуля віртуальної моделі периферійного пристрою, в якому актуальна інформація від самого периферійного пристрою, що змінюється на підставі наданої інформації. Далі отримана інформація візуалізує новий стан периферійного пристрою.

Програмне забезпечення є базовою платформою, для розгортання мережі IoT. Основними такими платформами є: Amazon Web Services, Microsoft Azure, ThingWorx IoT Platform, ThingWorx IoT Platform, Cisco IoT Cloud Connect, Salesforce IoT Cloud, Oracle Integrated Cloud[7].

Розглядаючи загальну архітектуру IoT–рішень, треба акцентувати увагу на підключення віддалених пристроїв (датчиків) до хабу (HUB). Для швидкого масштабування IoT-мереж, використовується підключення по радіодоступу. Звідки виникають потребі по використання частотного діапазону. Це може буди ліцензований діапазон, або діапазон що не ліцензується на території України.

При використанні неліцензійного діапазону – можуть виникнути ризик с безпекою доступу, та перехоплення повідомлень, що передаються в радіоефірі. Також можливі радіозавади, від інших елементів електромагнітного коливання, які працюють в неліцензійному діапозоні.

IoT елементи, які використовують радіодоступ, до опорної точоки доступу IoT інфраструктури називаються – LPWAN мережею [6-8].

LPWAN (Low-Power Wide-Area Network) – це мережі радіодоступу, що застосовуються для пристроїв і великих бездротових мереж телеметрії. Особливостями LPWAN мереж - це низьке енергоспоживання (low-power) і широкий територіальне охоплення (wide-area). Це дозволяє забезпечувати енергоефективну передачу даних на великі відстані (до 10 км.), при цьому елементи живлення можуть працювати досить тривалий час.

На рисунку 2 наведена типова схема мережі LPWAN.

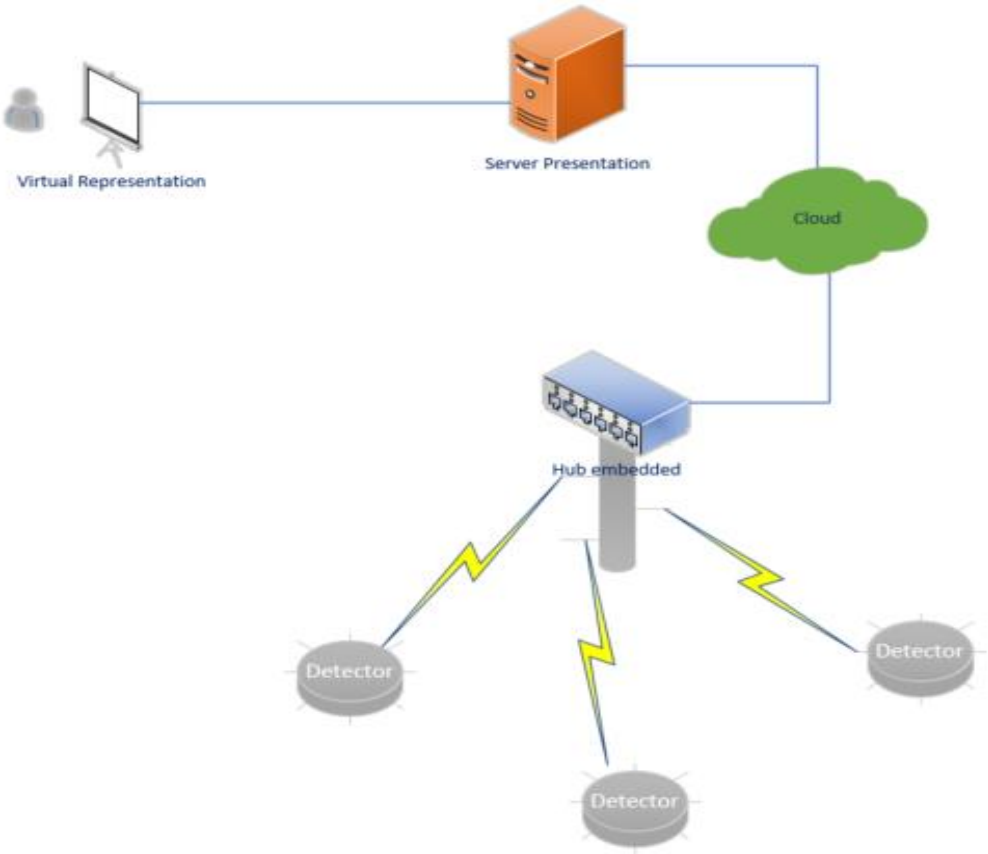

Рис. 2. Типова схема мережі LPWAN

В зв’язку з затребуваністю використання LPWAN мереж, виникають і ризики з доступністю мережі, збором даних, а також ризиками пов'язаними з передачею отриманих даних для аналізу,

або зберігання.

В останні роки дуже активно обговорюється питання безпеки таких мереж. Мережі інтернету речей, в тому числі LPWAN мережі потрапляють в групу ризику легкої-доступності, та проникнення несанкціонованого доступу. Це пов'язано з слабкими паролями, вразливим ПО, відсутність оновлень для обладнання, які вже підключені до пристроїв IoT .

За результаті американських досліджень, яке проводилося на базі виявленого шкідливе ПО відоме як VPNFilter, було скомпрометовано півмільйона маршрутизаторів, спонукавши Федеральне бюро розслідувань США (ФБР), порадити людям перезавантажити свої маршрутизатори [2].

Такого роду кібератаки можуть виходити в ході запуску пристрою Інтернету речей (IoT). Таким пристроєм може виступити, наприклад, камера відеоспостереження, або постійно включений датчик - який можуть постійно передавати дані, або в результаті якого можуть постійно генеруватися дані, для відправки в ядро мережі. Ситуація може посилиться, при постійній відправці таких даних, одночасно кілька десятків, або тисяч таких мережевих елементів IoT.

Проблематика даної ситуації, полягає в труднощі доказової бази неприродної складовою такої атаки, і навпаки доказ зовнішнього впливу на працездатність елементів мережі IoT. На даний момент, профільні фахівці можуть проводити аналіз і збір доказових даних виключно комп'ютерів і мобільних Smart-пристроїв (телефони, планшети) [2].

Національний інститут інформаційних і комунікаційних технологій Японії (NICT), аналізуючи всі кібератаки в Японії, за останні роки, - прийшов до висновку, що 54% атак були спрямовані на пристрої IoT, або з допомогою інфраструктури мережі IoT [4].

Результатом таких досліджень, Японія затвердила план з тестування безпеки, в який включила близько 200 мільйонів пристроїв Інтернету речей (IoT). Основною метою масштабного тестування, стало підвищення стійкості до кіберпростору. Першим етапом тестування стали приватні домашні мережі, які повинні забезпечувати сервіси безпеки.

Планується перевірка використання списку паролів, що встановлені виробниками обладнання, а також паролів, що найчастіше використовуються. Співробітники національного інституту інформаційних і комунікаційних технологій Японії (NICT) спробували увійти в випадково вибрані інтелектуальні гаджети, так званий тест на проникнення [4].

Другим етапом тестування стали оператори і провайдери інтернет-послуг (ISP), а також міські органи влади, через мережу яких можливе втручання в клієнтські (абонентські) пристрої. Додатково до другого етапу тестування, передбачається можливість повідомляти власників незахищених пристроїв, і допомагати їм заблокувати свої інтелектуальні пристрої.

Масштабний «пентест» було прийнято на законодавчому рівні і охоплює 5-ти річний період (до 2023 г.) [4].

Розуміючи таки ризики, треба унеможливити несанкціонованій доступ до приватних мереж. Одним із варіантів безпеки в приватних LPWAN мережах, може бути впроваджена стандарт NB-IoT.

NB-IoT (Narrow Band) було розроблена на базі існуючих стандартів мобільного зв'язку. Мережі NB-IoT працюють в ліцензованому спектрі частот, та забезпечує значно краще покриття і проникнення, збільшує максимальну кількість підключених до мережі пристроїв. NB-IoT забезпечується підтримка до 100 тисяч з’єднань на одну базову станцію. Система живлення, що підключена до датчика NB-IoT, може працювати до десяти років без підзарядки.

Для того, щоб краще зрозуміти можливості рішень на базі IoT і NB-IoT їх треба порівняти, та оцінити, що є більш актуальне для автоматизації промислових сервісів:

1. Простота розгортання.

При розгортанні повноцінної мережі LTE, стандарт NB-IoT розгортається шляхом програмного оновлення існуючих базових станцій, щоб запустити сервіси NB-IoT.

Рішення IoT (на базі обладнання LoRaWAN, Sigfox, GoodWan) - це стандарти протоколу

LPWAN, що працює в технологічному середовищі, які не є стільниковим стандартом. Для запуску такої мережі не потрібне отримання ліцензій на використання частот [6].

2. Синхронізація.

Мережа NB-IoT працює за принципом мобільного зв'язку, тому пристрої, що працюють в ній, повинні «прокидатися» і синхронізуватися з мережею. В іншому випадку отримати, або відправити повідомлення не вдасться.

Устаткування в мережі IoT (на базі обладнання LoRaWAN, Sigfox, GoodWan) - працює інакше. Асинхронна відправка даних (передача даних) виникає тільки тоді, коли ці дані є. Поки пристрою нічого передавати, він «спить», економлячи енергію. Програмно можна задавати відправку даних за розкладом.

3. Час автономної роботи.

Оскільки NB-IoT працює в ліцензованому спектрі частот, пристрої повинні синхронізуватися з мережею відносно часто. Це, в свою чергу, витрачає заряд батареї.

В архітектурі мережі IoT (на базі обладнання LoRaWAN, Sigfox, GoodWan) - синхронізація з мережею не потрібно. В асинхронних діапазонах, тільки фізичні зміни у кінцевого пристрою визначають, як довго пристрій може «спати».

4. Швидкість передачі даних.

Середня швидкість передачі даних в мережах NB-IoT - 200 Кбіт/с, в мережах IoT - від 300 біт/с до 50Кбіт в секунду. NB-IoT - це більш ефективний протокол IoT для «швидших» додатків.

5. Пропускна смуга.

NB-IoT зазвичай працює на більш високої пропускної здатності, ніж мережах IoT. Вимоги до пропускної здатності сигналу, позначені в стандарті 3GPP, складають 180 кГц. У мережах IoT потрібно лише 125 КГц.

6. Покриття мережі.

NB-IoT найкраще працює в складних міських районах. Продуктивність мережі буде надлишкової в приміських, або сільських районах. Мережі IoT не покладається на передачу великих обсягів даних. В зв’язку з цим, її покриття залишається відносно невеликим і стійким незалежно від умов місцевості.

7. Випадки застосування.

Мережі IoT підходять для додатків і пристроїв, які невибагливі до швидкостей передачі даних і до кількості даних, що відправляються. NB-IoT найкращим чином підходить для додатків, вибагливих до часу затримки (час затримки мінімальний) і регулярного прийому і відправлення повідомлень.

8. Сценарії розгортання.

Рішення IoT може використовуватися в приватних мережах без задіяння телекомунікаційного оператора. В Україні, NB-IoT можуть розвивати тільки мобільні оператори, але технологія має і сценарії автономного розгортання приватної мережі, без задіяння мобільних операторів.

9. Коефіцієнт витрат.

Загальна вартість модулів (датчиків) IoT дешевше в два рази аналогів в NB-IoT.

Висновки.

Описуючи процес роботи та взаємодії концепції інтернет речей, щодо їх можливостей та створення нових сервісів, необхідно однозначне розуміння кейсу застосування і сфери використання. Це розуміння буде напряму впливати на концептуальний підхід, щодо розгортання LPWAN, або NB-IoT рішень. Так само концепція розвитку IoT-рішень, вплине на бюджет витрат, при розгортання таких системи. Рішення на базі NB-IoT – це виклик промисловим підприємствам, які націлені на повну, або часткову автоматизацію. Інтерпрайс компанії – це розвиток напрямку NB-IoT. Саме таке рішення дозволять повну взаємодію M2M пристроїв, для виконання он-лайн процесів. Переваги приватних NB-IoT-мереж порівняно з

LPWAN полягають у підвищеній надійності та безпеки, а також більш низькому рівні затримки сигналів, що є однією з ключових вимог при віддаленому керуванні процесів підприємства.

Список використаної літератури

1. Колюбякин В. «Беспроводные мультисервисные сети»- М.: Теле-спутник. 2016.
2. Tomas Foltyn. Global police test their cyber-chops in simulated IoT attack - https://www.welivesecurity.com/2018/03/05/interpol-test-iot-simulated-attack/
3. Davis J. et al. Smart manufacturing, manufacturing intelligence and demand-dynamic performance // Davis J./ Computers & Chemical Engineering. – 2012. – Т. 47. – С. 145-156.
4. Tomas Foltyn. Japan to probe citizens' IoT devices in the name of security https://www.welivesecurity.com/2019/01/31/japan-probe-citizens-iot-security/
5. Perry Lea «Architecture internet of things», 2018.
6. Сети для IoT :LPWAN. Сетевые решения, 2016.
7. Top Eight IoT Platforms to Watch in 2019 Top-IoT-platforms \\sam-solutions.com/blog/top-eight-internet-of-things-platforms/
8. Ericsson Mobility Report \\ www.ericsson.com/en/mobility-report?

References

1. Kolyubyakin V. (2016) *"Wireless multiservice networks"*, M., Satellite TV.
2. Tomas Foltyn. Global police test their cyber-chops in simulated IoT attack - *https://www.welivesecurity.com/2018/03/05/interpol-test-iot-simulated-attack/*
3. Davis J. et al. (2012) "Smart manufacturing, manufacturing intelligence and demand-dynamic performance", *Computers & Chemical Engineering,* Vol. 47: 145-156. Print.
4. Tomas Foltyn. Japan to probe citizens' IoT devices in the name of security *https://www.welivesecurity.com/2019/01/31/japan-probe-citizens-iot-security/*
5. Perry Lea (2018) "Architecture internet of things". Print.
6. Networks for IoT: LPWAN. *Network solutions,* (2016). Print.
7. Top Eight IoT Platforms to Watch in 2019 Top-IoT-platforms *https://sam-solutions.com/blog/top-eight-internet-of-things-platforms/*
8. Ericsson Mobility Report *https:// www.ericsson.com/en/mobility-report?*

Автори статті (Authors of the article)

Сорокін Денис Володимирович – аспірант, асистент кафедри Комп'ютерної інженерії (Sorokin Denys Volodymyrovych – Postgraduate Student, Assistant of Department of Computer Engineering,). Phone: +380 (63) 282 68 13. E-mail: deny.sorokin@gmail.com.

Бондарчук Андрій Петрович – д.т.н., директор інституту інформаційних технологій (Bondarchuk Andrii Petrovych – D.Sc. in Technics, Director of the Institute of Information Technologies). Phone.: +380 (97) 408 61 31. E-mail: 0-99@i.ua.

Сторчак Каміла Павлівна – д.т.н., завідувач кафедри інформаційних систем та технологій (Storchack Kamila Pavlivna – D.Sc. in Technics, Head of the Department of Information Systems and Technologies). Phone.: +38(044) 249 25 42. E-mail: kpstorchak@ukr.net.