Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

АТЕСТАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Метод ідентифікації пристроїв IoT
на базі архітектури цифрових об'єктів

(тема)

Виконав:
студент II курсу, групи СПм-19-1
Явніков Р.Д.
(прізвище, ініціали)

Спеціальність
123 – Комп'ютерна інженерія
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма
Системне програмування
(повна назва освітньої програми)

Керівник: доц. Токарєв В.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 – Комп'ютерна інженерія
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20___ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові Явнікову Роману Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Метод ідентифікації пристроїв IoT
на базі архітектури цифрових об'єктів

затверджена наказом по університету від " 30 " жовтня 2020 р. № 1486 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 14 грудня 2020 р.

3. Вхідні дані до роботи Метод Ерлана
Система резолюцій DO – Handle system
Можливість роботи з інтерфейсом Wi-Fi.
Операційна система – Windows 10.
Технічне забезпечення: IBM - сумісний комп'ютер, AVR – мікроконтролер – 328P .
Представлення вихідних даних: згідно нормативних документів.

4. Перелік питань, що потрібно опрацювати в роботі
1) огляд літератури за темою роботи
2) аналіз предметної області
3) вибір та обґрунтування методики дослідження
4) проведення експериментальних досліджень
5) висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Демонстраційні матеріали. Плакати – № 18 - арк. ф. А4

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд літератури за темою роботи	03.11.20 - 20.11.20	
2	Вибір та обґрунтування методики дослідження	21.11.20 - 24.11.20	
3	Вибір інструментальних засобів	25.11.20 - 01.12.20	
4	Проведення експериментів	02.12.20 - 05.12.20	
5	Оформлення матеріалів атестаційної роботи	06.12.20 - 11.12.20	
6	Подання атестаційної роботи керівникові та її	14.12.20 - 15.12.20	
	попередній захист		
7	Подання атестаційної роботи на рецензування	16.12.20	

Дата видачі завдання 02 листопада 2020 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Токарєв В.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка атестаційної роботи: 77 с., 21 рис., 3 табл., 1 дод., 14 джерел.

БЕЗДРОТОВА МЕРЕЖА, ІНТЕРНЕТ, ПРОТОКОЛ, СЕРВЕР, IoT HANDLE SYSTEM, GPS, WI-FI, WLAN.

Метою атестаційної роботи є розробка методу ідентифікації пристроїв IoT на базі архітектури цифрових об'єктів.

У ході виконання атестаційної роботи розглядаються розробки моделей і методів ідентифікації пристроїв і додатків IoT. Були отримані нові результати, які дозволили розглянути можливі сценарії впровадження ідентифікації на базі архітектури цифрових об'єктів та запропонувати технічні рішення щодо забезпечення сумісності з існуючими методами ідентифікації та функціонуванням в гетерогенних мережах.

ABSTRACT

Master’s thesis: 77 pages, 21 figures, 3 tables, 1 appendices, 14 sources.

WIRELESS NETWORK, INTERNET, PROTOCOL, SERVER, HANDLE SYSTEM, GPS, WI-FI, WLAN.

The purpose of the certification work is to develop a method for identifying IoT devices based on the architecture of digital objects.

During the validation work, the development of models and methods for identifying IoT devices and applications is considered. New results were obtained that made it possible to consider Possible scenarios for the implementation of identification based on the architecture of digital objects and to propose technical solutions to ensure compatibility with existing methods of identification and functioning in heterogeneous networks.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ГІС – геоінформаційна система

ІКТ – інфокомунікаційні технології

МЗЗК – мережі зв'язку загального користування

МСЕ – міжнародний союз електрозв'язку

СМО – система масового обслуговування

DOA – архітектура цифрових об'єктів (англ., Digital Object Architecture)

DOI – цифровий ідентифікатор об'єкта (англ., Digital Object Identifier)

GPS – глобальна система позиціонування (англ., Global Positioning System)

IDoT – ідентичність в IoT (англ., IDentity in the Internet of Things)

IMEI – міжнародний ідентифікатор мобільного устаткування (англ., International Mobile Equipment Identity)

IMSI – міжнародний ідентифікатор абонента (англ., International Mobile Subscriber Identity)

IoT – інтернет речей (англ., Internet of Things)

MPA – режим работы с несколькими основными администраторами (англ., Multi-Primary Administrators)

SWOT – метод стратегічного планування (англ., Strength Weakness Opportunities Threats)

WDS – бездротова розподільча система (англ., Wireless Distribution System)

ВСТУП

Інтернет речей (IoT – Internet of Things) є сучасною концепцією, що припускає об'єднання об'єктів, «речей», в єдину всесвітню мережу, яка дозволяє речам бути розумними для взаємодії як один з одним, так і з людиною в будь-який час і в будь-якому місці. На сьогоднішній день число пристроїв, підключених до мережі, перевищує число всіх жителів планети і продовжує стрімко збільшуватися, що піднімає питання про присвоєння кожному об'єкту унікальної адреси, забезпечення конфіденційності та безпеки при передачі даних. Незважаючи на це, до цих пір немає загальноприйнятого методу ідентифікації речей, який би задовольняв всім вимогам як для існуючих пристроїв і додатків Інтернету речей, так і для новостворюваних.

Ідентифікатор являє собою виділений, публічно відомий атрибут або ім'я (або набір атрибутів та імен) для окремого пристрою. Як правило, ідентифікатори діють в межах певної області або мережі, що ускладнює ідентифікацію речей в глобальному масштабі. Зважаючи на складність і високу продуктивність сучасних пристроїв Інтернету речей вони можуть мати більше ніж один ідентифікатор. У той же час, існують різні методи ідентифікації, які не можуть використовуватися багатьма пристроями IoT з різних причин. Сучасні методи анонімізації і величезне число пристроїв IoT, підключених до мереж зв'язку загального користування (МЗЗК), роблять сучасні мережі і системи зв'язку уразливими перед зловмисниками. Уразливість мережевої безпеки, що полягає в неможливості аутентифікації пристроїв IoT, відкриває для зловмисників можливість для виробництва контрафактних фізичних і віртуальних речей.

Одним з напрямків забезпечення гарантованої і однозначної ідентифікації пристроїв IoT є використання унікального ідентифікатора пристрою IoT в МЗЗК в сукупності з параметрами самого пристрою. У

зв'язку з цим однією з найважливіших проблем є вибір системи ідентифікації для всіх пристроїв IoT, підключених до МЗЗК. В якості унікального глобального ідентифікатора пропонується безліч різних програмних і апаратних рішень. Одним з рішень, яке задовольняє пропонованим вимогам щодо ідентифікації пристроїв і додатків Інтернету речей є архітектура цифрових об'єктів DOA (Digital Object Architecture). Архітектура цифрових об'єктів і її базова система резолюції "Handle system" була спочатку створена як система резолюції ідентифікаторів, що володіє достатньою гнучкістю використання. Ідентифікатори містять актуальну інформацію про об'єкт – розміщення, умови використання, ключі шифрування і т.д. Дворівнева система резолюції і розподілена архітектура технології дозволяє швидко відображати зміни властивостей об'єктів і використовувати власну бізнес-модель для кожного адміністратора і сервера.

У зв'язку з тим, що архітектура цифрових об'єктів найбільш повно задовольняє перерахованим вище вимогам, розробка моделей і методів для ідентифікації пристроїв і додатків IoT є досить актуальною.

1 АНАЛІЗ МЕТОДІВ ІДЕНТИФІКАЦІЇ ПРИСТРОЇВ І ДОДАТКІВ IoT

В даний час IoT є загальновизнаною концепцією розвитку мереж зв'язку в короткостроковій і довгостроковій перспективах, а також передовою платформою в рамках розвитку цифрового інтелекту в концепції «Розумна країна». На думку більшості консалтингових аналітичних компаній, протягом наступних п'яти років в кожній зі сфер життєдіяльності людини будуть присутні понад 25 мільярдів пристроїв. Таким чином, можна говорити про всепроникаючий характер проникнення IoT в наше повсякденне життя.

Як відомо, фраза IoT вперше прозвучала від Кевіна Ештона в 1999 році на презентації інноваційних рішень компанії «Проктер і Гембл». Ештон запропонував нанести RFID мітки на продукцію, що випускається компанією, і таким чином забезпечити її взаємодію з радіоприймачем (рисунок 1.1).

Кевін Ештон припустив, що такий збір даних може бути використаний для вирішення багатьох проблем в реальному світі.

В результаті в даний час багато пристроїв можуть обмінюватися даними через Internet, взаємодіючи зі смартфонами, один з одним і з аналогічними схожими пристроями.

У 2001 році дослідницький центр Auto-ID Массачусетського технологічного інституту, в якому працював Кевін Ештон, адаптував використання RFID міток для різноманітної продукції, місцезнаходження якої стало можливо відслідковувати через Internet.

У 2005 році термін "IoT" був офіційно використаний Міжнародним союзом електрозв'язку (МСЕ) в технічному звіті, присвяченому перспективним концепціям розвитку мереж зв'язку. В останнє десятиліття IoT став однією з проривних технологій, загальновизнаних усіма країнами

світу.

IoT дозволяє людям і речам взаємодіяти де завгодно, коли завгодно, і в будь-яких поєднаннях при використанні інфраструктури IoT. Екосистема IoT передбачає збір даних з датчиків (або відправку команд на виконавчі пристрої), їх передачу через мережу зв'язку на хмарні платформи для подальшого аналізу з метою надання інтелектуальних послуг для людей.

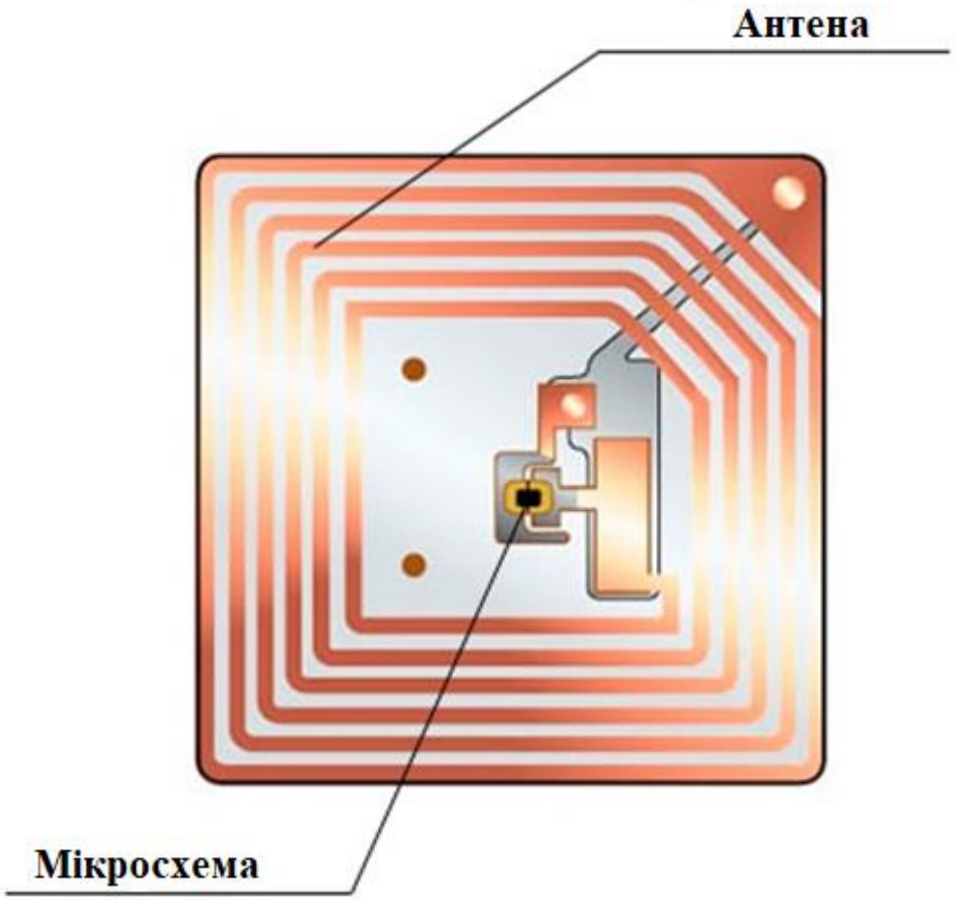

Рисунок 1.1 – Приклад RFID мітки

На рисунку 1.2 представлені ключові компоненти, необхідні для побудови систем IoT.

Згідно малюнку, датчики і пристрої знімання інформації збирають різні види даних про той чи інший об'єкт, потім ці дані можуть бути додатково оброблені та проаналізовані для отримання корисної інформації з метою

надання інтелектуальних послуг.

Елементи IoT зведені в одну просту формулу:

Фізичні об'єкти + контролери, сенсори, виконавчі механізми +
+Інтернет = IoT.

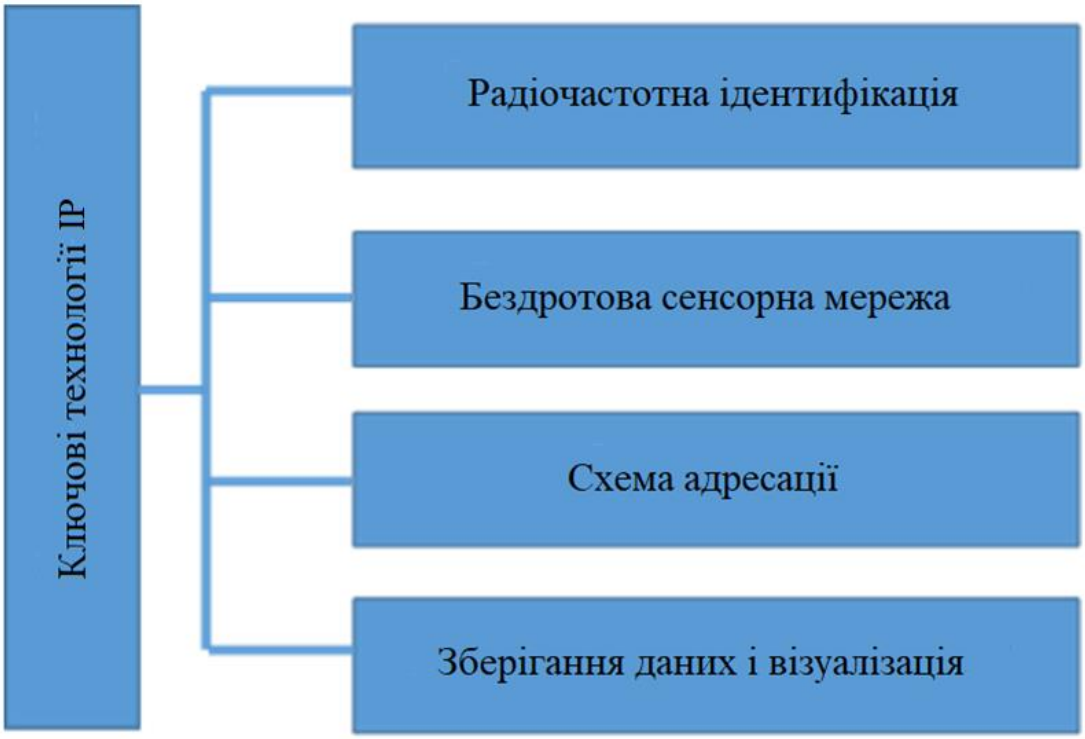

Рисунок 1.2 – Основні компоненти IoT

Існують різні додатки IoT, які спрямовані на вирішення конкретних завдань.

Серед типових додатків можна виділити:

- управління даними;
- аналітику;
- візуалізацію;
- управління гетерогенними мережами;
- дослідницькі цілі та ін.

Тим щонайменше, дослідження IoT все ще продовжують перебувати в

зародковому стані, зважаючи на існування багатьох невирішених проблем, наприклад, проблем, пов'язаних з часом автономної роботи, простотою «легковагості» технологій передачі даних, виконанням дій в залежності від контексту того, що відбувається, питаннями ідентифікації та безпеки, вартості кінцевих пристроїв, масштабованості і гетерогенності. Незважаючи на всі переваги IoT останнім часом з'явилися випадки розкриття даних, зібраних пристроями IoT, що змушує турбуватися про ідентичність пристроїв і додатків в рамках концепції IoT. Дійсно, ідентифікація відіграє важливу роль в IoT. Наприклад, зловмисники можуть використовувати портативні RFID / NFC- зчитувачі для крадіжки персональних даних з банківських карт в громадському транспорті, використовуючи вразливості технології типу PayPass (рисунок 1.3).

Рисунок 1.3 – Приклад технології PayPass

Це можливо завдяки відсутності підтвердження особи власника RFID-зчитувача. Іншим прикладом є можливість перехоплення зловмисником даних мереж пристроїв IoT з метою отримання IMEI-ідентифікаторів (рисунок 1.4), різних кінцевих пристроїв, оснащених модемами, з метою

подальшої широкомовної розсилки навмисно спотворених повідомлень. Поточні рішення, відомі у всьому світі, спрямовані, в основному, на прив'язку пристрою або програми IoT з ідентифікатором, подібною IP-адресою або номером мобільного телефону, за яким можна зрозуміти: хто користується тим чи іншим пристроєм.

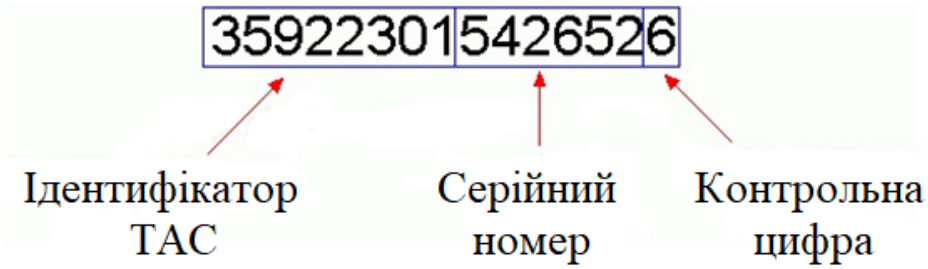

Рисунок 1.4 – Приклад IMEI-ідентифікатора

Дослідження в цій області були розпочаті в результаті обговорення цих проблем в регулюючому органі BEREC (Body of European Regulators for Electronic Communications). У той же час, ідентифікація має набагато ширші масштаби і є більш доречною для безлічі додатків і сутностей (суб'єктів) в IoT.

1.1 Класифікація ідентифікаторів для IoT

На сьогоднішній день ідентифікатори використовуються для різних цілей в додатках IoT.

Основним завданням ідентифікатора, який присвоюється тій чи іншій речі, є ідентифікація, що дозволяє однозначно визначати речі і бути цільовими сутностями додатків IoT. Крім ідентифікації речей, ідентифікації також підлягають:

- додатки;
- послуги;

- користувачі;
- дані;
- кінцеве обладнання;
- протоколи;
- місця знаходження речей.

1.1.1 Ідентифікатор речей

Ідентифікатор речі визначає цільову сутність додатка IoT. Це може бути, наприклад, будь-який фізичний об'єкт (обладнання, приміщення, люди, тварини, рослини) або цифрові дані (файл, набір даних, метадані), тобто що завгодно, з чим можна взаємодіяти в реальному і віртуальному світі (рисунок 1.5).

Рисунок 1.5 – Приклад ідентифікатора речей

Приклади використання ідентифікаторів речей:

- предиктивне обслуговування. Компанії можуть надавати послуги по предиктивному обслуговуванню їх продуктів (наприклад, електроприводи, виробниче обладнання). Продукти, при цьому, повинні мати вбудовані сенсори і інтерфейси для комунікації. Сервіс по предиктивному обслуговуванню розташовується в хмарному сервісі. З'єднання з обладнанням на території клієнта здійснюється через захищене з'єднання (наприклад, VPN) за допомогою мережевого з'єднання клієнта або за допомогою мобільного Інтернет з'єднання. Продукт має вбудований в незалежну пам'ять ідентифікатор, за допомогою якого устаткування і визначається на хмарній платформі;

- відстеження майна. Компанії можуть стежити за власним майном (великого і малого розмірів, рухомим і нерухомим) шляхом регулярної перевірки його розташування. В даному випадку, будь-яке майно має власний ідентифікатор об'єкта, виконаний у вигляді штрих-коду, QR- коду або RFID-мітки. Отримані мітки підлягають постійному скануванню персоналом компанії за допомогою ручного сканера, який здійснює з'єднання з сервером. З кожним скануванням супроводжуюча інформація про майно може бути надана за допомогою інтерфейсу сканера, призначеного для користувача;

- походження і контроль якості відстежуваної інформації. Наступний приклад показує важливість чіткого визначення об'єкта. Вантажна логістична компанія маркує товар, що транспортується, за допомогою міток RFID. Дані мітки містять ідентифікатор об'єкта транспортуємого продукту спільно з будь-якими іншими атрибутами (виробник, дата виробництва та ін.). Місцезнаходження продукту записується при проходженні пунктів зчитування. Надалі, дані мітки можуть бути повторно використані для інших продуктів з іншим ідентифікатором об'єкта. Мітка сама по собі також зберігає власний ідентифікатор мітки, який використовується компанією для визначення походження інформації, контролю якості міток і ін. Прикладом

подібних ідентифікаторів, що зберігаються на одній мітці, але при цьому відносяться до різних сутностей, є електронний код продукту (Electronic Product Code, EPC), а також ідентифікатор мітки (Tag Identifier, TID), визначений міжнародною організацією GS1. Електронний код продукту ідентифікує продукт, до якого прикріплена мітка, в той час як ідентифікатор мітки – ідентифікує безпосередньо мітку. На відміну від ідентифікатора мітки, який не змінюється протягом життя, електронний код продукту змінюється з кожним новим продуктом, до якого мітка прикріпляється.

1.1.2 Ідентифікатор додатків і послуги

Ідентифікатори додатків і сервісів визначають додатки і сервіси, що також включають в себе способи взаємодії з додатком або сервісом (наприклад, НИД на малюнку 1.6). Портал HID потрібен для реєстрації користувачів і їх мобільних пристроїв, а також для випуску / відкликання мобільних ідентифікаторів.

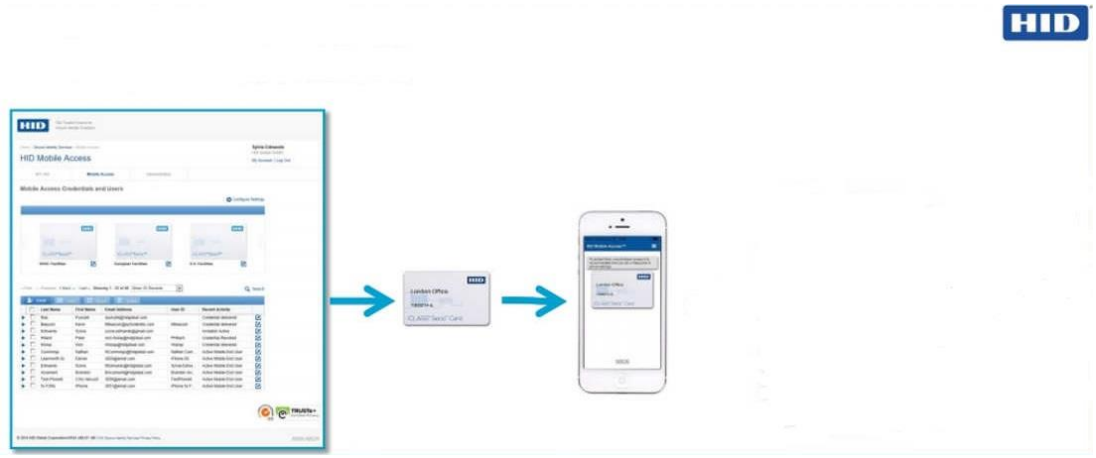

Рисунок 1.6 – Приклад отримання мобільних ідентифікаторів

Приклади використання ідентифікаторів додатків і сервісів, послуги на базі платформ IoT. Платформа IoT може надавати різні сервіси, наприклад, сервіс забезпечення зв'язку, магазин додатків, сервіс управління пристроями,

сервіс реєстрації пристроїв. Кожний сервіс має унікальний ідентифікатор. Сервіси можуть бути занесені до реєстру, що дозволить додаткам здійснювати пошук сервісів. Сервіси також можуть бути представлені додаткам. Для федеративних платформ (як правило, функціонуючих в межах країни), в випадках, коли один і той же сервіс (наприклад, сервіс реєстрації) може бути надано різними (наприклад, регіональними) програмними платформами, можливо привласнення безлічі унікальних ідентифікаторів для певного числа послуг одного і того ж типу.

1.1.3 Комунікаційні ідентифікатори

Комунікаційні ідентифікатори визначають кінцеве комунікаційне обладнання (наприклад, джерело або одержувач), а також сесії.

Приклади використання ідентифікаторів зв'язку. Грунтуючись на прикладі, описаному в документі ETSI GS LTN 002 Європейського інституту по стандартизації в галузі телекомунікацій, енергоефективні мережі далекого радіусу дії (Low Power Area Networks, LPWAN), використовують унікально присвоєні комунікаційні ідентифікатори для визначення кінцевого обладнання в межах кожної з мереж (рисунок 1.7).

Централізовані центри обслуговування обмінюються даними з кінцевим обладнанням через точки доступу в обох напрямках. Кінцеве обладнання зареєстровано в системі за допомогою унікального комунікаційного ідентифікатора. При встановленні з'єднання від терміналу до сервісу обслуговування, кінцеві пристрої використовують власні комунікаційні ідентифікатори в якості адреси відправника з метою подальшої успішної обробки і маршрутизації пакета до центрального сервісу.

У разі з'єднання відбувається запит від сервісу обслуговування до терміналу. Кінцеві пристрої запитують в мережі існуючі дані, використовуючи власний комунікаційний ідентифікатор в якості адреси одержувача.

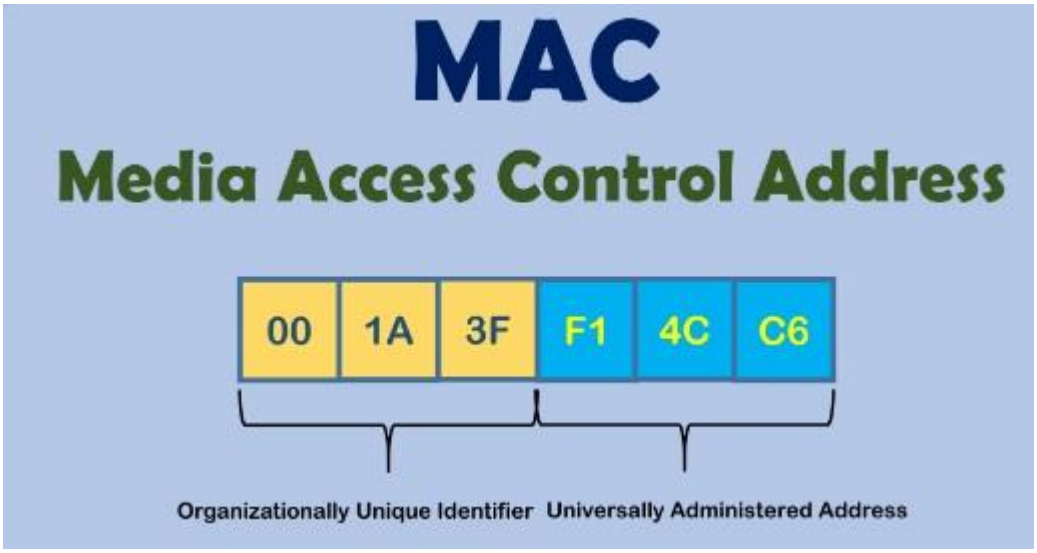

Рисунок 1.7 – Приклад комунікаційного ідентифікатора

1. Ethernet/WiFi MAC адреса. У мережах на основі технологій Ethernet / WiFi (прик. IEEE 802.3) MAC адреса є ідентифікатором для комунікаційного кінцевого обладнання на канальному рівні. MAC-адреса пристрою призначається виробником обладнання. Дана адреса складається з 48 біт (6 байт), де перші 3 байти позначають унікальний ідентифікатор організації (Organizationally Unique Identifier, OUI), який призначається компаніям реєструючим органом IEEE (Інститут інженерів електротехніки та електроніки).

2. IP-адреса. Адреси IPv4 і IPv6 (прик. IETF RFC 4291) використовуються в мережах IP для логічної ідентифікації кінцевого обладнання на мережевому рівні. Розмір адреси IPv4 дорівнює 32 бітам, в той час як розмір адреси IPv6 дорівнює 128 бітам. IP адреса буває глобальна (публічна), локальна або типу Link-local, в залежності від сфери застосування і використовуваної мережі. Більш того, підтримуються також адреси для широкомовної, багатоадресної і одноадресної розсилки (broadcast, multicast, unicast). IP-адреси структурно засновані на принципі маршрутизації і складаються з мережевого префікса і ідентифікатора інтерфейсу, розмір яких може варіюватися. Глобально унікальний діапазон IP-адреси розподілений

між п'ятьма основними регіональними інтернет-реєстраторами (Regional Internet Registries, RIRs), який в подальшому може розподілятися між інтернет-провайдерами на безпосередньо призначені для користувача мережі. Управління глобальним набором адрес здійснюється реєстром доменів верхнього рівня (IANA), який і виділяє блоки IP-адрес регіональним інтернет-реєстраторам.

3. Телефонний номер. Телефонні номери присвоюються конкретному пристрою абонента в телефонній мережі. Залежно від сфери застосування, можуть використовуватися глобально і локально унікальні номери. Для дзвінків за допомогою локального номера в глобальну мережу використовується номер з розширенням, що надає глобальну унікальність. Глобальний телефонний номер починається з коду країни, визначеним Міжнародним Союзом Електрозв'язку. Коди регіонів або провайдерів призначаються регулюючими організаціями в конкретній країні.

4. Сесія HTTP. Комунікаційною сесією можна вважати обмін серією пов'язаних між собою повідомлень. Прикладом може бути інтернет-магазин, в якому користувач може наповнити кошик декількома позиціями і потім здійснити оплату. Веб-серверу необхідно відстежувати всі дії користувача в контексті магазину. Протокол HTTP не надає механізмів щодо збереження стану, тому необхідно зберігати виділений ідентифікатор сесій, щоб надавати подібний функціонал магазину. Ідентифікатор генерується сервером і звичайно зберігається в якості спеціального фрагмента даних на стороні клієнта, який є параметром в запитах HTTP GET и POST.

1.1.4 Ідентифікатор користувача

Ідентифікатор користувача однозначно визначає користувача сервісу або додатку Інтернету речей. Користувачем може бути людина, компанія (юридична особа) або навіть програмне забезпечення, яке взаємодіє з відповідними додатками Інтернету речей. Приклади використання

ідентифікаторів користувачів на рисунку 1.8.

Рисунок 1.8 – Приклад ідентифікатора користувача

1. Користувач-людина. З метою отримання певної інформації від пристрою, що здійснює управління пристроями інтернету речей, людині необхідно авторизуватися в системі. Для цього спочатку людині необхідно ідентифікувати себе в системі, наприклад, за допомогою імені користувача, спеціальної чіп-карти або відбитка пальця. Залежно від системи безпеки, можлива аутентифікація додатковими методами. Система перевіряє наявність прав доступу у конкретного користувача до об'єктів або сервісів Інтернету речей і проводить необхідні дії. Права користувача залежать від групи, до якої він належить. Усередині системи Інтернету речей, користувачеві призначається особливий ідентифікатор, який прив'язується до всіх операцій, пов'язаними з безпекою, і який може відрізнятися від ідентифікатора, що використовується людиною для власних ідентифікацій.

2. Програмний доступ до об'єктів IoT. У певних сценаріях можлива взаємодія програмного забезпечення додатків з об'єктом IoT за допомогою системи IoT. Додаток представляє себе системі у вигляді певного ключа. Система перевіряє наявність необхідних прав у додатка для здійснення доступу до об'єкта IoT і виконання необхідних дій.

1.1.5 Ідентифікатор даних

Даний клас покриває одночасно ідентифікацію особливих видів даних і типів даних (наприклад, метадані, властивості, класи) (рисунок 1.9).

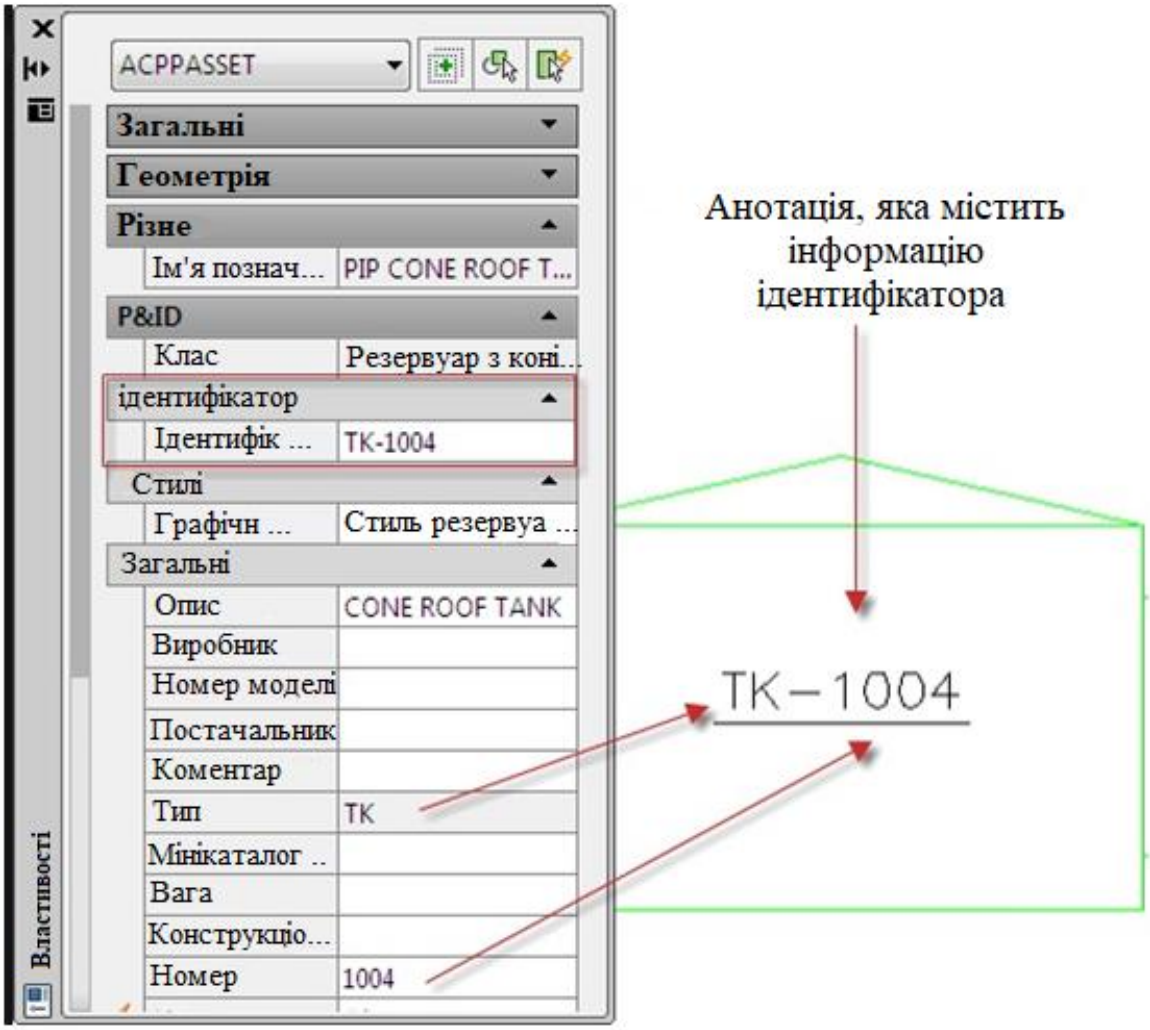

Рисунок 1.9 – Приклад ідентифікатора даних

Приклади використання ідентифікаторів даних.

1. Цифровий близнюк. Цифровий близнюк – це набір даних, що містить віртуальне уявлення про об'єкт. Він пов'язаний з річчю через ідентифікатор об'єкта. Більш того, з метою звернення і здійснення доступу з сервісів і додатків, сам цифровий близнюк також потребує ідентифікатор. Однак, сама річ може мати безліч цифрових близнюків, які, в свою чергу, можуть містити різні набори інформації.

2. Набір даних часового ряду. Збір даних з сенсорів пристрою Інтернету речей відбувається автоматично з постійною частотою. Дані зберігаються в якості тимчасового ряду безпосередньо на платформі Інтернету речей для подальшого використання. Різні додатки можуть здійснювати доступ до цих даних, наприклад, для інтелектуального обслуговування, оптимізації процесів або прогнозів. Набір даних потребує особливого ідентифікатора, який би дозволив звертатися до таких даних з додатків.

3. Типи властивостей об'єктів. Властивості об'єкта, такі як вага, розміри і температура, є стандартизованими для певних цілей використання. Визначення властивостей включає значення, діапазон значення, формат конкретної властивості. Кожне з подібних визначень має потребу в унікальному ідентифікаторі з метою однозначного звернення до таких.

1.1.6 Ідентифікатор місцезнаходження

Даний розділ розглядає ідентифікацію розташування в географічних районах (координати в просторі, поштові адреси, номери кімнат) (рисунок 1.10).

Приклади використання ідентифікаторів місцезнаходження.

1. Відстеження продуктів. Компанія може відстежувати доставку товарів високої вартості. GPS-приймач з модемом для передачі даних по мережі є частиною транспортного впакування. GPS-координати упаковки

передаються з періодичними інтервалами в хмарний додаток, що відстежує шлях руху продукту.

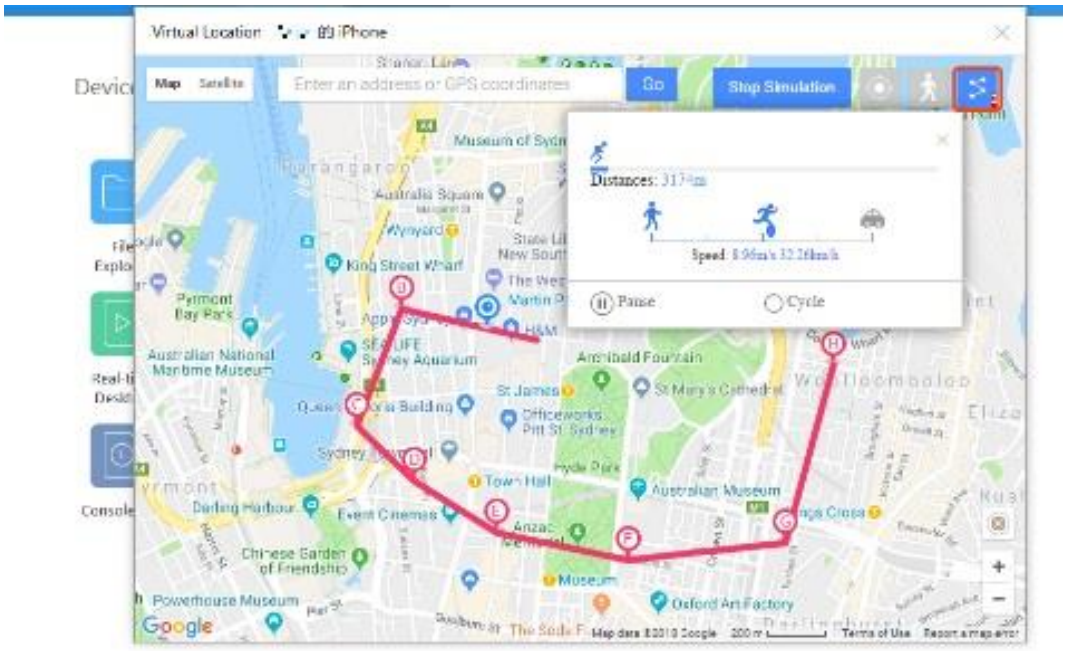

Рисунок 1.10 – Приклад ідентифікатора місцезнаходження

2. Обслуговування нерухомості. Керівник об'єкта повинен контролювати своєчасне обслуговування систем нагріву, вентиляції та кондиціонування (HVAC) на великих територіях. Системи HVAC сповіщають про аварійні ситуації, що використовується спільно з сервісами інтелектуального обслуговування. З метою супроводу обслуговуючого персоналу до необхідного місця аварії, в кожне з пристроїв необхідно вбудувати ідентифікатор, який прив'язує пристрій до певної локації (наприклад, будівля, поверх, номер кімнати).

1.1.7 Ідентифікатор протоколу

Ідентифікатори протоколів можуть інформувати, наприклад, комунікаційні протоколи про протоколи верхніх рівнів, дані яких вони

передають з нижніх рівнів, або також можливо здійснити сповіщення додатків про протоколи, які краще використовувати для здійснення необхідного обміну даними.

1.2 Категорії вимог для ідентифікаторів в IoT

Варто відзначити, що більшість вимог не обмежені конкретним ідентифікатором класу або набором класів. Унаслідок різного рівня детальності, а також розмаїття природи представлених вимог, категорії вимог визначені і деталізовані. Приклади по кожній з категорії вимог зведені воєдино, відповідно до стандарту AIOTI WG03:

- унікальність. Вимоги по унікальності ідентифікаторів в залежності від області застосування сильно розрізняються. Багато хто чекає глобальної унікальності, в той час як деякі обмежують унікальність до локальної, або до локальної в межах домену продавця або виробника. Також, з причин конфіденційності, в одному з варіантів використання пропонувалося не використовувати унікальність зовсім. Окремою темою для обговорення є спосіб забезпечення унікальності ідентифікаторів, що знаходяться під управлінням різних організацій.

- конфіденційність і захист особистих даних. Конфіденційність є основою в темах, пов'язаних з взаємодією людей і їх особистих даних. Дана тема пов'язана з ідентифікаторами користувачів, які безпосередньо визначають конкретних людей, а також ідентифікаторів для сутностей, які можуть бути дуже близько пов'язані з людьми і їх діяльністю. Наприклад, автомобіль, особисте обладнання, товари, розташування, адреси для взаємодії (комунікації) кожного з яких належать або призначені конкретній людині (користувачеві) або обладнанню в його володінні.

- безпека. Вимоги безпеки найчастіше пов'язані безпосередньо з ідентифікатором, але в деяких випадках також очікується забезпечення безпеки даних, пов'язаних з ідентифікатором (пов'язаних з сутністю,

ідентифікованої за допомогою ідентифікатора). Забезпечення безпеки даних, пов'язаних з ідентифікатором, не розглядається в даному документі. Необхідно забезпечити коректну ідентифікацію сутності за допомогою ідентифікатора, виключити підробку в процесі виділення сутності з безлічі інших, під час переміщення і використання. Призначення підпису для ідентифікатора вказується як один з головних способів досягнення даної цілі. Дублювання і використання ідентифікатора для інших сутностей повинно бути виключено. Перевірка правильності ідентифікатора повинна бути доступна через глобальну мережу, а також у разі відсутності Інтернет-з'єднання.

- аутентифікація ідентифікатора також є бажаною функцією, тому що потрібен спосіб довести приналежність ідентифікатора до правильної суті. Даний функціонал відноситься до функціоналу системи управління ідентифікацією і не описується в даному документі.

1.3 Стандарти ідентифікаторів

На даний момент проводиться безліч робіт по стандартизації ідентифікаторів, одночасно з уже існуючою безліччю стандартів в цій галузі. Розробляються все нові і нові документи, в яких враховується специфіка пристроїв і додатків IoT.

Більшість з них застосовувана тільки для певних сфер діяльності або сценаріїв застосування.

Стандарти ідентифікації часто застосовуються до більш ніж одного класу ідентифікаторів.

В рамках атестаційної роботи неможливо врахувати всі наявні на сьогоднішній день ідентифікатори, але буде наведено перелік стандартів і рекомендацій, які так чи інакше мають відношення до IoT.

Повний перелік був би корисний лише в тому випадку, якщо б ми могли використовувати ці стандарти для забезпечення сумісності і

актуальності в рішеннях IoT для кожного стандарту.

Однак, це не представляється можливим у зв'язку з величезною кількістю пересічних стандартів з обмеженим доступом, а також через обсяг роботи, який необхідно виконати для детального аналізу.

Замість цього, для кожної категорії ідентифікаторів в контексті IoT представлені приклади стандартів. Також варто відзначити, що це не означає, що обрані стандарти є кращими або обов'язковими до застосування.

Варто відзначити, що крім стандартів ідентифікації певних організацій по розробці стандартів, державними органами визначені ідентифікатори для певних цілей використання, наприклад, номери соціального страхування і номери автомобілів.

Також, компанії можуть мати власні «реалізації» поняття «ідентифікатор», подібно до серійних номерів у продуктів.

1.3.1 Стандарти ідентифікації речей

Існує велика кількість стандартів для ідентифікації речей. Найчастіше вони визначені для специфічних сфер або специфічних типів сутностей, але деякі з них використовуються в безлічі сфер застосування і для різних типів і класів сутностей.

Деякі стандарти надають механізми для схем множинної ідентифікації, що дозволяють реалізувати міжмережеву взаємодію всередині одного і того ж додатку Інтернету речей. Даний механізм відноситься до схем мета-ідентифікації.

Приклади.

1. VIN-номер автомобіля (Vehicle Identification Number), ISO 3779, визначає універсальну систему номерної ідентифікації для автомобілів.

2. Кодування вантажних контейнерів, ідентифікація та маркування визначені в стандарті ISO 6346. Надає систему ідентифікації з обов'язковим маркуванням для візуальної інтерпретації та опціональні можливості для

автоматизованої ідентифікації та електронного обміну даними, а також система кодування для даних, яка залежить від типу і розміру контейнера.

3. Ідентифікація тварин на базі радіочастотних міток визначена в стандарті ISO 11784, незалежно від протоколу передачі між міткою і зчитувачем.

4. Ідентифікація RFID-міток за допомогою системи присвоєння унікальних ідентифікаторів визначена в стандарті ISO/IEC 15963. Ідентифікатор мітки (Tag ID, TID) може використовуватися для відстеження та контролю стану самої мітки. Також може бути використаний для відстеження об'єкта, до якого мітка прикріплена. Вважається хорошою практикою ідентифікувати об'єкти незалежно від технології передачі даних.

5. Юридичні особи також можуть бути ідентифіковані унікальним глобальним номером за допомогою унікального ідентифікатора юридичної особи (Legal entity identifier, LEI), визначеному в стандарті ISO 17442. Стандарт розроблявся для застосування в контексті послуг фінансового сектора. Тим не менш, він також може бути використаний для будь-яких випадків, де необхідно посилатися на юридичну особу.

6. Цифровий ідентифікатор об'єкта (Digital Object Identifier, DOI) визначено в ISO 26324 з метою ідентифікації сутностей в Інтернеті і використовується в основному для надання доступу до об'єкта, спільноти чи для управління інтелектуальною власністю.

Система DOI спочатку була спроектована для забезпечення сумісності і роботи з існуючими системами ідентифікації, а також схемами метаданих. В атестаційної роботі розглядаються моделі і методи ідентифікації пристроїв і додатків Інтернету речей на базі архітектури цифрових об'єктів. Далі більш детально буде описана взаємодія основних елементів цієї архітектури.

В даний час відсутні дослідження, в яких була б докладно представлена архітектура цифрових об'єктів як новий механізм для ідентифікації пристроїв і додатків IoT. Роботи зі стандартизації методів ідентифікації пристроїв і боротьби з контрафактом на базі архітектури цифрових об'єктів в даний час

ведуться в дослідницькій комісії МСЕ-Т. Міжнародний союз електрозв'язку (МСЕ, англ. International Telecommunication Union, ITU) – міжнародна організація, що визначає рекомендації в галузі телекомунікацій та радіо, а також регулює питання міжнародного використання радіочастот (розподіл радіочастот з призначень та по країнах). Заснований як Міжнародний телеграфний союз в 1865 році, з 1947 року є спеціалізованою установою ООН. Сектор стандартизації електрозв'язку Міжнародного союзу електрозв'язку, ССЕ МСЕ) – підрозділ Міжнародного союзу електрозв'язку, розробляє технічні стандарти з усіх міжнародних питань цифрового та аналогового зв'язку і займається вирішенням технічних та поточних питань, а також питань, пов'язаних з тарифікацією. З 1995 року офіційна англійська назва – ITU-T. Так, в грудні 2018 року на процедуру згоди була представлена Рекомендація «Архітектура взаємодії пристроїв інтернету речей на базі архітектури цифрових об'єктів», а в 2019 році – Рекомендація «Структура рішень по боротьбі з контрафактними пристроями інтернету речей на базі архітектури цифрових об'єктів».

Проведений аналіз показав, що перспектива повсюдного застосування архітектури цифрових об'єктів створить унікальні умови для транснаціональної єдиної системи ідентифікації, яку вже сьогодні необхідно впроваджувати у новостворювані пристрої та додатки IoT.

1.4 Загальна концепція архітектури цифрових об'єктів

Як було показано в попередніх параграфах, існуючі системи ідентифікації і управління інформацією в мережі засновані на класичній клієнт-серверній архітектурі (рисунок 1.11). Сервер в такій системі є місцем зберігання інформації і обробки запитів від клієнтів на роботу з даною інформацією. DOA, на відміну від такого підходу прагне вирішити питання не про локалізацію, а про контекст цифрового об'єкта.

Рисунок 1.11 – Приклад архітектури цифрового об'єкта

Цифровий об'єкт в цій архітектурі характеризується не тільки інформацією про своє місцезнаходження. Крім цього, існує можливість отримувати різні відомості про сам об'єкт:

- вимоги до доступу;
- аутентифікації;
- інформацію про автора та інше.

Вся ця інформація вноситься самим творцем цифрового об'єкта. Для цього в архітектуру DOA інтегрована спеціальна інфраструктура, що забезпечує необхідне шифрування і верифікацію доступу.

Основними структурними елементами DOA є цифровий об'єкт, система резолюції ідентифікатора (Handle System) та репозиторій і реєстр цифрових об'єктів. Зупинимося на принципах система резолюції докладніше.

Кожному цифровому об'єкту в описуваній архітектурі ставиться у відповідність унікальний ідентифікатор – DOI (від англ. Digital Object Identificator). Даний ідентифікатор чимось нагадує URL, на базі якого побудований сучасний Інтернет. Однак, на відміну від останнього, присвоювані ідентифікатори залишаються постійними і не залежать від стану цифрового об'єкта. Саме система резолюції пов'язує ідентифікатор з

інформацією про поточний статус цифрового об'єкта (місцезнаходження, доступ, інформація про автентичність).

У класичній архітектурі DOA система резолюції є дворівневою:

- першим рівнем резолюції є глобальний реєстр (GHR, від англ. Global Handle Registry);

- другим рівнем – набір локальних реєстрів (LHR, от англ. Local Handle Registry) або локальних сервісів (LHS, від англ. Local Handle Service).

Для дозволу ідентифікатора в даній підсистемі, спочатку йде звернення до глобального реєстру GHR, який повідомляє інформацію про локальний реєстр LHR, в якому міститься необхідна інформація про цифровий об'єкт.

Сама структура ідентифікатора DOA також відповідає дворівневій системі. Наприклад, розглянемо ідентифікатор: 10.1000 / 123abc. Перша частина, розташована до «/», носить назви префікса; друга частина – суфікса. Префікс дозволяє встановити відомості про локальний реєстр цифрового об'єкта LHR. Дана відповідність префікса та інформації про адміністратора зберігається в глобальному реєстрі GHR. Суфікс вже однозначно ідентифікує конкретний об'єкт, і дана інформація, що зв'язує суфікс з конкретним об'єктом зберігається в локальному реєстрі LHR.

2 АНАЛІЗ СИСТЕМИ ІДЕНТИФІКАЦІЇ АРХІТЕКТУРИ ЦИФРОВИХ ОБ'ЄКТІВ

Архітектура цифрових об'єктів (Digital Object Architecture – DOA) і пов'язана з нею система резолюцій Handle System були розроблені корпорацією національних дослідницьких ініціатив (CNRI) на початку 1990-х років, грунтуючись на роботах над цифровими бібліотеками для Управління перспективних дослідницьких проектів Міністерства оборони США (DARPA). Одним з початкових мотивів створення DOA була необхідність ідентифікації та отримання інформації про об'єкт протягом тривалого періоду часу (порядку десятків або сотень років).

Розробка архітектури цифрових об'єктів стала спробою переходу від представлення даних в Інтернеті за допомогою наборів вузлів і транспорту до виявлення і доставці інформації у вигляді цифрових об'єктів.

Мета створення архітектури цифрових об'єктів – вирішення наступних проблем управління цифровою інформацією:

- забезпечення стандартного доступу до розрізненої інформації (ідентифікація, пошук інформації і надання даних, забезпечення безпеки, типізація);
- взаємодія з різноманітними інформаційними системами;
- незалежність від конкретних базових технологій, які використовуються для розміщення та обслуговування інформації;
- взаємодія протягом тривалих періодів часу;
- активне управління системами, на яких поширюється інформація;
- забезпечення великого рівня масштабованості;
- розподілена архітектура;
- відкрита архітектура;
- стандартні протоколи і процедури взаємодії компонентів системи.

Архітектура цифрових об'єктів – архітектура розподіленої системи

зберігання, визначення місця розташування і пошуку інформації в Internet (рисунок 2.1).

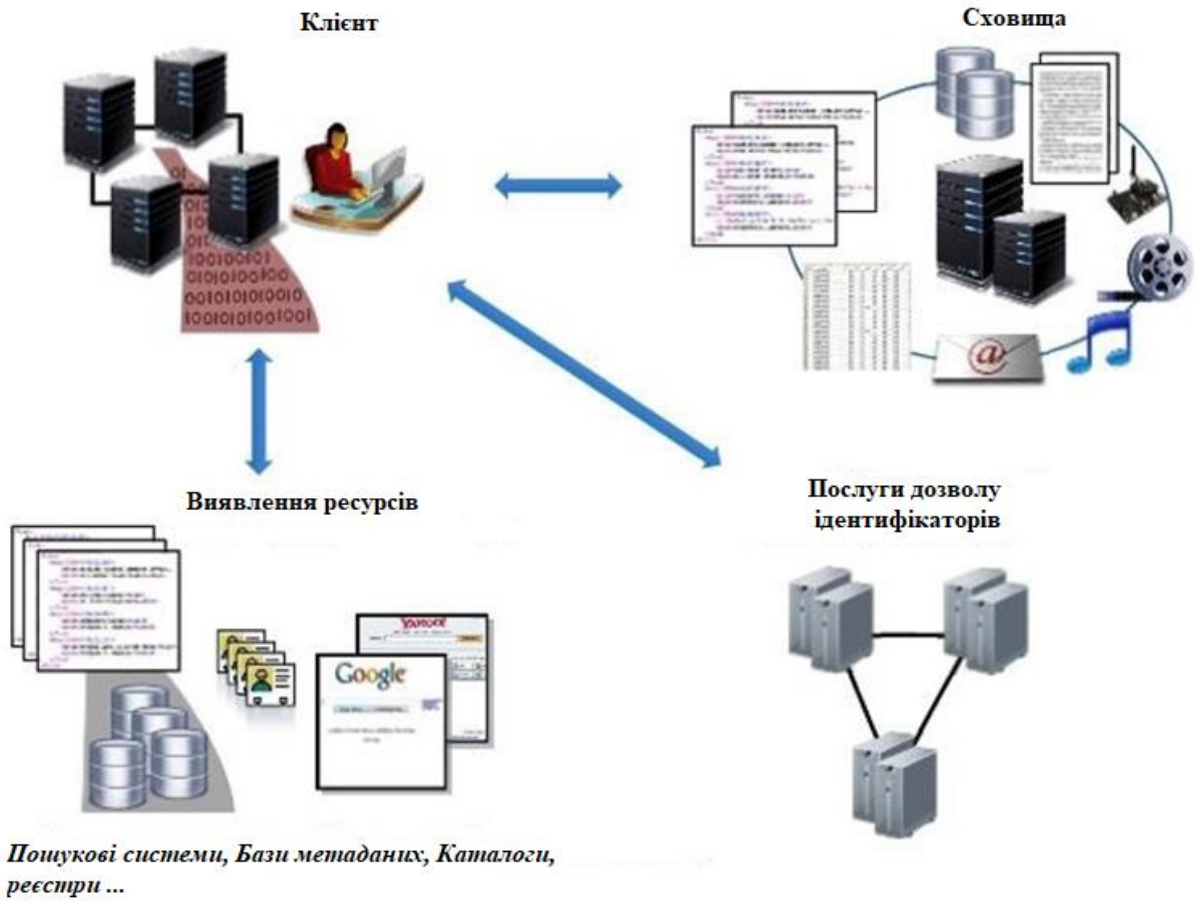

Рисунок 2.1 – Фундаментальні компоненти архітектури цифрових об'єктів

Кожен об'єкт в цілому має набір ознак, що визначають його сутність і, завдяки цьому, виділяють його з безлічі інших. Таким чином, різні ознаки будуть свого роду унікальними ідентифікаторами.

Ідентифікація необхідна для вирішення таких завдань, як:

- однозначне визначення об'єкта;
- розпізнавання об'єкта за його властивостями;
- групування об'єктів за певними ознаками;
- виділення об'єкта з безлічі подібних.

Згідно Рекомендації МСЕ-Т X.1255, цифровий об'єкт – це «структура виявлення інформації по управлінню визначенням ідентичності», загальноприйнята структура даних, що складається з одного або декількох елементів, завдяки якій забезпечується функціональна сумісність інформаційних систем в Інтернеті.

За фактом, цифровий об'єкт – це об'єкт, що складається з структурованої послідовності біт, що має: назву, унікальний ідентифікатор і атрибути, які описують його властивості. Однак, в ідентифікації цифрових об'єктів виникає складність, тому що людина сприймає не самі біти, а їх відображення за допомогою програмного забезпечення.

Таким чином, чим більше в цьому процесі задіюється сенсорний апарат людини, тим суб'єктивніше питання, що саме вважати сутністю цифрового об'єкта і розглядати способи його ідентифікації.

В контексті DOA, цифровий об'єкт – дані, що не залежать від платформи. Для управління цифровими об'єктами використовуються три архітектурних компонента.

Кожен з компонентів може використовуватися самостійно, але в комбінації вони забезпечують розподілену і масштабовану систему управління інформацією в Internet. Такими компонентами є:

- масштабована і розподілена система ідентифікаторів і резолюцій цифрових об'єктів;
- репозиторії доступу і управління цифровими об'єктами;
- реєстри для пошуку і виявлення об'єктів.

Система резолюції пов'язує ідентифікатори з інформацією про стан цифрових об'єктів. Наприклад, така інформація може містити місцезнаходження даного об'єкту в Інтернеті або вимоги до доступу, інформацію про аутентифікацію і т.п. Створювач об'єкта або авторизований адміністратор надає цю інформацію з використанням інфраструктури публічних ключів, яка інтегрована в DOA. Технологія публічних ключів передбачає використання двох ключів для шифрування – публічного і

приватного.

Цифрові об'єкти – ключовий елемент, навколо якого побудовані інші компоненти і сервіси.

Цифрові об'єкти не замінюють існуючі формати і структури даних, але забезпечують загальноприйняті способи подання цих форматів і структур. Це дозволяє їх однозначно інтерпретувати і переміщати між різними гетерогенними інформаційними системами в ході змін в системах з часом.

В контексті Рекомендацій MCE-T об'єктами можуть бути мережі, сервіси, документи, права доступу, транспортна інформація, пристрої або окремі чіпи, авторські твори або будь-яка інша інформація, представлена у вигляді структури даних і пов'язаних з ними метаданих, тобто у вигляді цифрового об'єкта.

Таким чином, в якості цифрового об'єкта можна уявити і будь-який об'єкт реального світу.

З кількох розглянутих вище визначень можна зробити висновок що цифровий об'єкт – структурований запис, що містить дані, інформацію про стан даних і метаданих.

Цифровий об'єкт може містити покажчики на місця, де може бути знайдена відповідна інформація.

Всі цифрові об'єкти доступні з використанням протоколу цифрових об'єктів, незалежно від основних технічних систем.

Кожен цифровий об'єкт описує себе і свій вміст. Кожен цифровий об'єкт містить в собі опис своїх власних правил управління доступом.

2.1 Система резолюції

Система резолюції (Handle System) була створена, щоб подолати обмеження функціональності існуючих систем ідентифікації об'єктів в Інтернеті. Резолюція – це процес, в якому ідентифікатор є запитом до мережевого сервісу на отримання актуальної інформації (даних про стан), що

відноситься до обумовленої суті (найчастіше мова йде про місцезнаходження).

Система резолюції підтримує множинну резолюцію, тобто відповіддю на запит може бути розташування різних примірників об'єкта, пов'язані сервіси і будь-яка інша інформація, зазначена в метаданих об'єкта. Інформація, що повертається, необов'язково повинна вказувати на екземпляр об'єкта: наприклад, це може бути опис або стан об'єкта, деякі індикатори або вимірювання, відносини з іншими сутностями і т.д.

Хэндел – глобально унікальний і розв'язний ідентифікатор. Він представляється в такий спосіб: «префікс / суфікс», де префікс унікальний в межах Системи резолюції. Приклад Хендел зображений на рисунку 2.2.

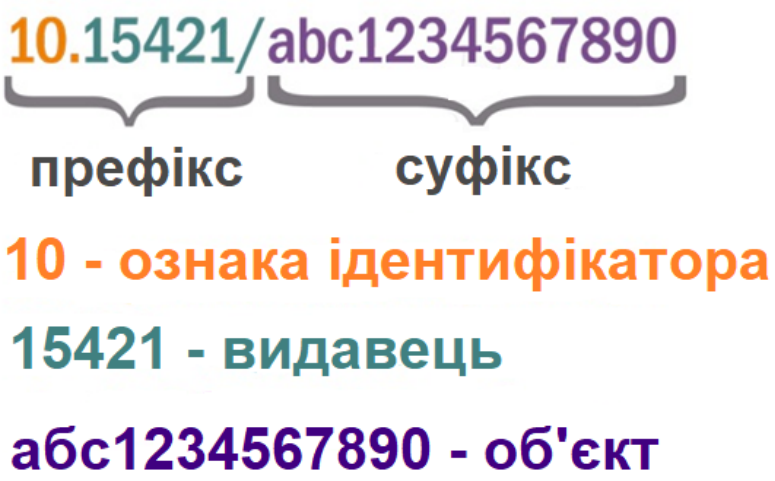

Рисунок 2.2 – Приклад хендела

Система резолюції надає доступ клієнта до місця розташування цифрового об'єкта. Для цього використовується ієрархічна модель обслуговування, що складається з глобального реєстратора Хендел GHR, від (англ. Global Handle Registry) (GHR) і локальної системи обробки Хендел LHS від (англ., Local Handle Registry) (LHR). Кожна служба локальної дескрипції може містити свою власну ієрархію Хендел сервісів: GHR містить інформацію про зіставлення префікса Хендел для LHS, який обслуговує

Хендел для даного префікса.

На рисунку 2.3 зображено приклад ідентифікатора «bar.foo/1234». Префікс верхнього рівня «bar», службова інформація якого міститься в LHS A.

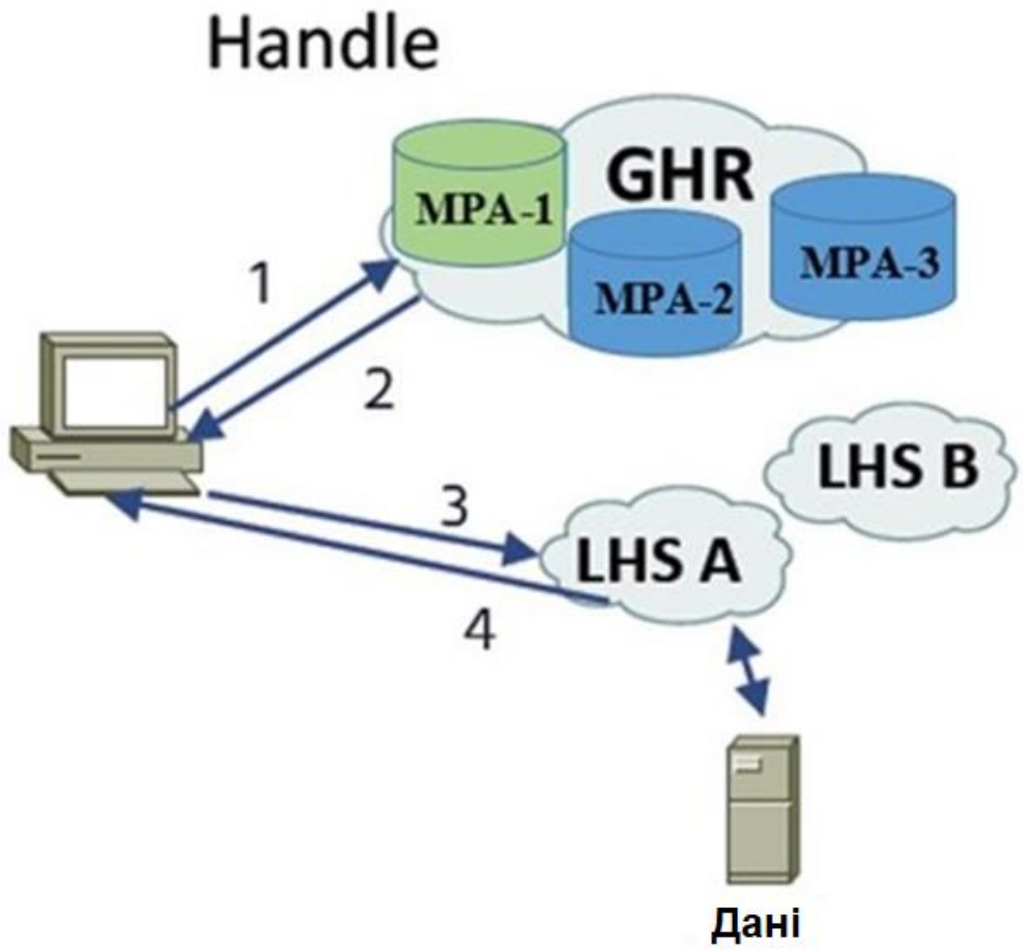

Рисунок 2.3 – Резолюція ідентифікаторів

GHR відповідає за управління коренем ієрархії дескрипторів системи, виділяючи унікальні префікси і надаючи глобальну службу прив'язки префіксів до LHS цього префікса.

Кожному об'єкту в системі резолюції приписаний ряд обов'язкових атрибутів:

- числовий ідентифікатор даних (індекс);

- тип даних. Тип даних являє собою посилання на запис в системі резолюції;
- час останньої зміни даних;
- час життя записів в системі TTL (Time To Live);
- права доступу для адміністратора запису і для неавторизованого користувача;
- посилання на адміністратора даного запису про об'єкт;
- посилання на інші хендели;
- дані.

В протоколі HSP – Handle System Protocol передбачений ряд можливостей для уточнення одержуваного набору даних:

- вибір типу даних, що повертаються;
- вибір індексу або діапазону індексів;
- вказівка на те, чи можна відповісти кешованими даними.

Таким чином, система Handle System:

- забезпечує базову систему ідентифікаторів в Інтернет;
- ідентифікатор містить дані про поточний стан об'єкта;
- ідентифікатор зберігається, навіть якщо місце розташування та інші атрибути об'єкта змінюються;
- має високу масштабованість;
- пов'язує одне або кілька типізованих значень, наприклад, IP- адреса, відкритий ключ, URL-адресу кожного ідентифікатора;
- володіє відкритим, чітко визначеним протоколом взаємодії і моделлю даних;
- забезпечує інфраструктуру для доменів додатків, наприклад, цифрових бібліотек і публікацій, електронних досліджень і т.д.

Основними якостями, закладеними при її створенні, були:

- унікальність – кожен хендел унікальний в рамках глобальної системи;
- постійність – хендел можуть використовуватися в якості постійних

ідентифікаторів для об'єктів в Інтернеті. При цьому хендел не залежить від об'єкта, який він називає, їх єдиний зв'язок – в самій системі;

- множинні екземпляри – хендел може вказувати на різні екземпляри ресурсу, які розташовані по різним мережним адресам;

- множинні атрибути – хендел може вказувати на різні атрибути ресурсу, включаючи пов'язані сервіси, які розташовані по різним мережним адресам;

- розширюваний простір імен – локальний простір імен можна приєднати до глобального, отримавши статус реєстратора і унікальний префікс, щоб уникнути конфліктів з існуючими іменами;

- модель безпеки – система резолюції дозволяє здійснювати безпечну резолюцію і адміністрування;

- розподілений адміністративний сервіс – для кожного хендела в системі можна визначити власного адміністратора (власника);

- ефективний сервіс резолюції – протокол системи спроектований з урахуванням множинних одночасних звернень.

Інформація, яка повертається, не обов'язково повинна вказувати власне на екземпляр об'єкта: наприклад, це може бути опис або стан об'єкта, деякі індикатори або вимірювання, відносини з іншими сутностями і т.д. Для обробки запиту через протокол http система використовує проксі-сервери, які обробляють хендели, представлені у вигляді URL. Варіанти резолюції при цьому зберігаються в хендл-записи у вигляді xml-файлу. Таким чином, проксі-сервери, є надбудовою над системою резолюції.

2.2 Представлення системи ідентифікації на базі архітектури цифрових об'єктів

В даний час в результаті швидкого розвитку інформаційних технологій, зростання обсягів різноманітної інформації в мережі зв'язку загального користування (МЗЗК), а також через повсюдне впровадження технологій

інтернету речей з'явилася нагальна потреба впровадження механізмів однозначної ідентифікації пристроїв і додатків інтернету речей, що дозволяють відслідковувати достовірність інформації в мережі і боротися з контрафактною ІКТ-продукцією. Для розробки такого сервісу спочатку необхідно вибрати найбільш оптимальну систему ідентифікації. Для ідентифікації можна використовувати безліч різних програмних і апаратних рішень, наприклад, системи апаратної ідентифікації IPv6, зв'язку IPv4 + MAC, IMEI і ін.

Однак загальними недоліками цих систем є можливість програмної і апаратної зміни ідентифікатора мережевого інтерфейсу і прив'язка до апаратних ідентифікаторів, яка виключає можливість ідентифікації цифрового контенту, що відноситься до віртуальних сутностей інтернету речей і теж вимагає ідентифікації.

Цих недоліків позбавлені альтернативні програмні рішення для ідентифікації, такі як DOA, URI, XRI, IRI і ін., які дозволяють ідентифікувати будь-який віртуальний або реальний об'єкт в мережі зв'язку загального користування, незалежно від наявності або відсутності у нього мережевого інтерфейсу.

Ці системи так само, як і системи апаратної ідентифікації, використовують для аутентифікації фізичних і цифрових об'єктів різні сторонні технології. Крім того, необхідно відзначити, що не всі існуючі системи ідентифікації об'єктів відповідають розвитку мереж зв'язку в рамках концепції IoT.

Вибір оптимальної системи визначається наступними вимогами до технологій ідентифікації, які враховують її використання в МЗЗК:

- системи ідентифікації повинні відповідати на множинні запити;
- для роботи з ідентифікаторами необхідно реалізувати різні рівні доступу, тобто систему авторизації користувачів;
- база, яка містить дані, повинна бути відокремлена від самого об'єкта ідентифікації;

- ідентифікатори не повинні містити динамічні елементи або метадані.

На рисунку 2.4 представлена загальна архітектура для системи резолюції Handle System.

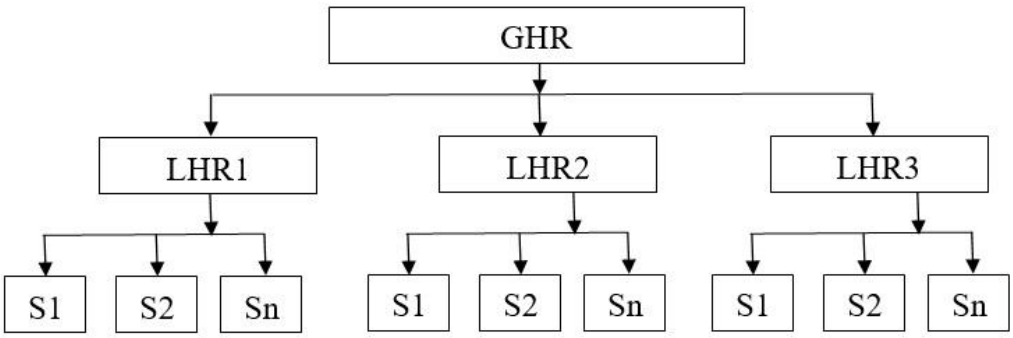

Рисунок 2.4 – Загальна архітектура для системи резолюції Handle System

Клієнт відправляє запит Handle в GHR. GHR повертає службову інформацію, яка вказує на систему LHR, управляючу префіксом ідентифікатора. Клієнт запитує LHR. LHR ідентифікує сервер, в результаті чого відбувається звернення до цифрового об'єкту, а в якості відповіді повертається запитувана клієнтом інформація.

Після цього клієнт обробляє отриману інформацію. GHR відповідає за управління коренем ієрархії дескрипторів системи, виділяючи унікальні префікси і надаючи глобальну службу прив'язки префіксів до LHR.

Реорганізація моделі управління DOA, яка проходить зараз, передбачає перехід від моделі з одним головним адміністратором GHR (до недавніх пір їм була CNRI) до моделі з декількома адміністраторами верхнього рівня MPA (Multi-Primary Administrator - багатоцільовий первинний адміністратор мережі цифрових ідентифікаторів), яких авторизує і чию діяльність координує некомерційна організація The DONA Foundation, зареєстрована в 2014 р в Женеві (Швейцарія).

Спільне технічне рішення, засноване на зв'язці IoT – ідентифікатор

DOA, може розглядатися як ефективний технологічний ланцюжок. У модуль, який взаємодіє з мережевою інфраструктурою, може бути записаний ідентифікатор DOA, до складу якого будуть включені всі унікальні параметри того чи іншого об'єкта (метадані). Додатки такого рішення можуть бути найрізноманітніші:

- інформаційно-комунікаційні технології (ІКТ);
- фармацевтична і автомобільна промисловості;
- авіабудування і т.д.

Зокрема, вони можуть використовуватися для боротьби з контрафактом.

Взаємодія елементів в рамках DOA передбачає комунікації між розподіленими LHR-серверами, розташованими в різних країнах. Однак розподіленість призводить до збільшення мережевої затримки, величина якої може виявитися неприйнятною для сервісів і додатків, що вимагають ультрамалих затримок на мережах зв'язку.

Для мінімізації мережевої затримки системи ідентифікації цифрових і фізичних об'єктів пропонується розбити систему резолюцій, ввівши регістри проміжного рівня між GHR і розподіленими LHR. Ці проміжні регістри можна також назвати середніми регістрами – MHR (від англ., Middle Handle Register) – (MHR). Кожний MHR може бути прив'язаний до певного географічного регіону на карті світу з урахуванням щільності та кількості розташованих там пристроїв, а також щільності виробників (тобто щільності LHR). LHR взаємодіє з найближчим MHR замість вилученого GHR, що зменшує відстань передачі даних по каналах зв'язку і, як наслідок, знижує мережеву затримку.

Рисунок 2.5 ілюструє структуру системного рівня з новими MHR. Вибір оптимальної кількості MHR і їх географічного розподілу – це завдання оптимізації, яка повинна бути вирішена з точки зору загальної вартості системи і параметрів якості обслуговування мереж зв'язку.

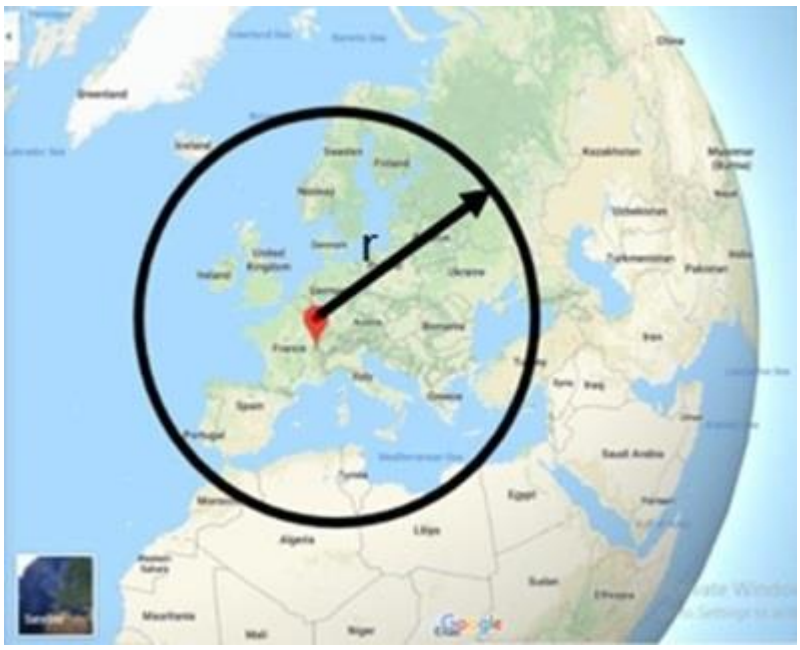

Рисунок 2.5 – Поточне місце розташування GHR і очікувані місця розташування MHR

3 МАТЕМАТИЧНА МОДЕЛЬ ПОБУДОВИ АРХІТЕКТУРИ ЦИФРОВИХ ОБ'ЄКТІВ З ПРОМІЖНИМ РІВНЕМ ВЗАЄМОДІЇ

Система має основний регістр (глобальний Регістр GHR), розташований в місті Женева. Для розробки моделі розташування глобального регістра GHR позначимо G (l, h, φ, λ), де l і h абсциса і ордината місця розташування GHR; φ, λ – широта і довгота GHR. GHR з'єднується з усіма проміжними (середніми) регістрами MHR, розгорнутими в системі.

Множину MHR представимо як $M_j(l_j, h_j, \varphi_j, \lambda_j)$ $j = 1, 2, ..., N$ де $l_j, h_j, \varphi_j, \lambda_j$ – відповідно абсциса, ордината, широта і довгота j-го проміжного регістру, а N – загальна кількість регістрів MHR, розгорнутих в системі.

Кожний проміжний регістр MHR з'єднується з групою локальних регістрів LHR і керує ними. Регістри LHR, пов'язані з j-м MHR, утворюють множину $(L_i^j(l_i^j, h_i^j, \varphi_i^j, \lambda_i^j))$, де i=1,2,…, M_j – де $l_j, h_j, \varphi_j, \lambda_j$ – абсциса, ордината, широта і довгота i-го регистра LHR, зв’язаного з j-м MHR, а M_j – загальна кількість локальних регістрів LHR, зв'язаних з j-м регістром MHR, розташованим в місці, яке описується координатами $l_j, h_j, \varphi_j, \lambda_j$.

Мережева затримка L між двома серверами прямо пропорційна відстані D між передавачем і приймачем:. У запропонованій системі, повідомлення передаються в основному між LHR і MHR.

Таким чином, мережева затримка для такої системи може бути розрахована наступним чином:

$$L_i^j \infty D_i^j .$$

$$D_i^j = \sqrt{(l_i^j - l_j)^2 + (h_i^j - h_j)^2}, \qquad (3.1)$$

де, L_i^j – це мережева затримка для даних, переданих між i-м LHR і j-м MHR;

D_i^j – відстань між передавачем i-го LHR і приймачем j-го MHR.

Пропонований підхід модифікованої системи регістрів був протестований на базі модельної мережі для перевірки продуктивності та зменшення мережевої затримки в порівнянні з існуючою системою регістрів.

Для моделювання був використаний програмний пакет Matlab. Припустимо, що пропонована система MHR містить N = 10 проміжних регістрів, які розташовані в різних країнах і працюють з усіма групами локальних регістрів LHR по всьому світу.

Таблиця 3.1 ілюструє спеціальні локації кожного проміжного регістра з широтою φ_j і довготой λ_j. Крім того, введемо апроксимовану відстань D_j^{GHR} між кожним проміжним регістром LHR і глобальним регістром GHR.

Таблиця 3.1 – Розташування проміжних регістрів MHR

n	Країна	Місто	Координата		Апроксимовані D_j^{GHR} відстані, км
			Широта, φj	Довгота, λj	
1	2	3	4	5	6
1	Україна	Київ	50,4502°N	30,5234°E	1854
2	Єгипет	Каір	30,0444°N	31,2357°E	4070,0
4	Іспанія	Мадрид	40,4168°N	33,7038°W	1384,1
5	США	Вашингтон	47,7511°N	120,741°W	8365
6	Китай	Гуанчжоу	23,1291°N	113,2644°E	9388
7	Італія	Рим	41,9028°N	12,4964°E	887,2
8	Бразилія	Бразилія	14,2350°S	51,9253°W	8866

Продовження таблиці 3.1

1	2	3	4	5	6
9	Канада	Кокран	51,2538°N	85,3232°W	6279
10	Австралія	Сидней	33,8688°S	151,2093°E	16764

Загальна кількість M_j локальних регистрів LHR, з'єднаних з кожним проміжним регістром MHR, представлена в таблиці 3.2.

Описи (специфікації) включають широту φ_j і довготу λ_j локації сервера LHR, апроксимовану відстань між кожним локальним регістром LHR і відповідним проміжним регістром MHR (D_i^j) і апроксимовану відстань D_j^{GHR} між кожним проміжним регістром LHR і основним регістром GHR.

Таблиця 3.2 – Розташування M1 локальних регістрів LHR, з'єднаних з проміжним регістром MHR1

n	Країна	Місто	Координата		Апроксимовані відстані, D (км)	Апроксимовані D_j^{GHR} відстані, км
			Широта	Довгота		
1	Фінляндія	Гельсинки	60,1699°N	24,9384°E	300,6	1980
2	Фінляндія	Тампере	61,4978°N	23,7610°E	397,3	2042
3	Україна	Київ	50,4501°N	30,5234°E	1055	1854
4	Турція	Анкара	39,9334°N	32,8597°E	2231	2267

4 МЕТОД ІДЕНТИФІКАЦІЇ ПРИСТРОЇВ ІОТ НА БАЗІ АРХІТЕКТУРИ ЦИФРОВИХ ОБ'ЄКТІВ

Одним з основних завдань перед інженерами стоїть надання доступу пристроїв IoT в Інтернет як безпосередньо, так і з використанням шлюзів. Це необхідно для того, щоб кожен об'єкт (інтернет річ) був віртуально або фізично представлений, мав адресу і був доступний через Інтернет в будь-який час і в будь-якому місці. В даний час розробка механізмів ідентифікації для різних класів і типів пристроїв триває як в Інтернеті речей, так і в Промисловому Інтернеті речей, а також є частиною досліджень в Міжнародних організаціях по стандартизації як державних, так і комерційних.

Існуючі механізми для ідентифікації, застосовувані в різних технологіях передачі даних, були придумані ще на рубежі століть, коли не піднімалося питання про передбачувану кількість пристроїв, що підключаються IoT.

Проведений аналіз показав, що можна створити ефективну схему привласнення унікальних ідентифікаторів тільки для дуже малої кількості пристроїв інтернету речей. Крім того, існуючі методи ідентифікації в більшості своїй не підтримують пристрої IoT, які короткочасно підключаються до мережі Інтернет, і що переміщаються між різними громадськими структурами і закритими мережами зв'язку. Також до недоліків даних методів можна віднести те, що в мережах зв'язку ідентифікатори можуть містити інформацію з прив'язкою до конкретного місця розташування пристроїв IoT. Об'єкти інтернету речей повинні мати ідентифікатори, які не залежать від того, в якій мережі вони знаходяться або яким користувачам належать. Інше питання, яке необхідно враховувати - це концептуальна різниця між ідентифікатором об'єкта і його мережевою адресою (або адресами). У найзагальнішому випадку ідентифікатор об'єкта і

його адреса різні і служать для різних цілей. Перший забезпечує унікальним ідентифікатором самий об'єкт, але мережева адреса може змінюватися в залежності від фізичного розташування об'єкта, його логічного членства в одній або декількох мережах або ролі того чи іншого об'єкта.

У випадках, коли ідентифікатор об'єкта і його адреса різні, ідентифікатор зазвичай структурований різними схемами ідентифікації. Електронний код продукту (EPC) є однією з добре відомих схем ідентифікації об'єктів, які можуть однозначно ідентифікувати об'єкти, пов'язані з RFID-міткою.

Інша схема ідентифікації, яка називається – повсюдно поширеним кодом (uCode), введена центром uID в Японії, представляє собою іншу систему кодування, яка підтримується виключно в Японії та Азії. Аналогічним чином і інші схеми адресації можуть бути різними. Об'єкти, які в даний час підключені до Інтернету, використовують глобальну схему IP-адресації (IPv4 або IPv6). У свою чергу деякі пристрої IoT не можуть використовувати глобальну IP-адресацію, з огляду на те, що підключаються до Інтернету через так званий шлюз.

Шлюзом, наприклад, може бути смартфон, який взаємодіє зі смарт-годинами за допомогою технології Bluetooth Low Energy. На рисунку 4.1 представлена схема такої взаємодії на прикладі сервісу фітнес трекінгу.

Одним з напрямків забезпечення гарантованої ідентифікації пристроїв і додатків IoT є архітектура цифрових об'єктів DOA. Переваги DOA в порівнянні з наявними системами ідентифікації очевидні:

- перевагою системи Handle в порівнянні з системою DNS є більш гнучка модель адміністрування префіксів і найкраща масштабованість при збільшенні кількості суфіксів в обраному префіксі;
- унікальність – кожен хендл унікальний в рамках глобальної системи;
- сталість – хендлом можуть використовуватися в якості постійних ідентифікаторів для об'єктів в інтернеті. При цьому хендл не залежить від об'єкта, який він називає, їх єдиний зв'язок - в самій системі. Це дозволяє

ідентифікатору існувати незмінним незалежно від змін місця розташування, володіння і т.д. Тобто при переміщенні ресурсу досить оновити його значення в Handle System для відображення нового місця розташування;

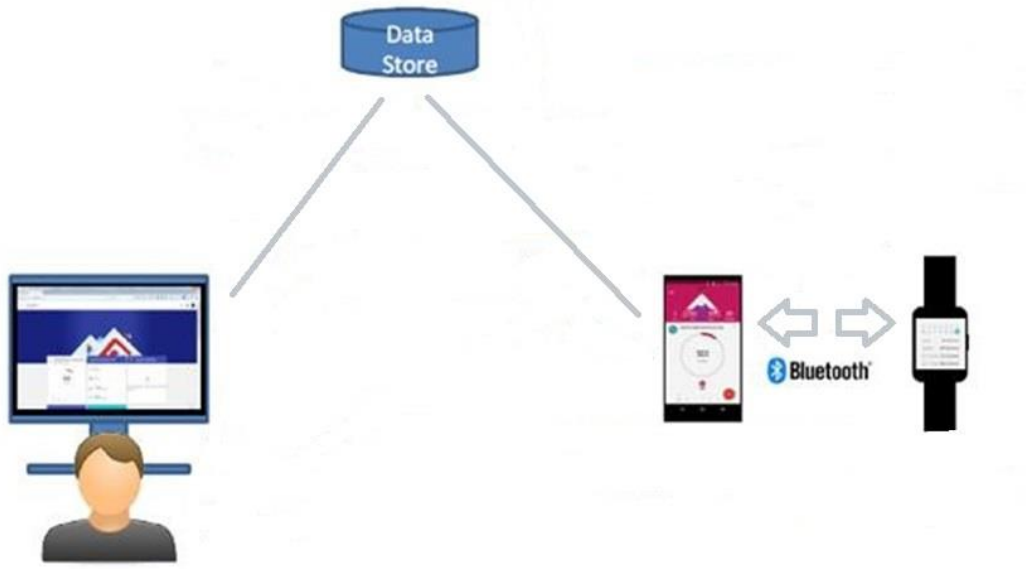

Рисунок 4.1 – Взаємодія ідентифікаторів в разі використання фітнес-трекінгу

- множинні екземпляри - хендл може вказувати на різні екземпляри ресурсу, розташовані по різним мережевим адресам. Додатки можуть використовувати цю якість системи для підвищення продуктивності і стійкості;

- множинні атрибути – хендл може вказувати на різні атрибути ресурсу, включаючи пов'язані сервіси, розташовані по різним мережевим адресам;

- розширюваний простір імен – локальний простір імен можна приєднати до глобального, отримавши статус реєстратора і унікальний префікс, щоб уникнути конфліктів з існуючими іменами. Використання реєстраторів дозволяє делегувати сервіси адміністрування та резолюції локальним сервісам (local handle service), яким буде передавати запити глобальний реєстр (Global Handle Registry), створюючи розподілену модель;

- модель безпеки - Handle System дозволяє здійснювати безпечну резолюцію і адміністрування. Протокол системи визначає стандартні механізми клієнтської і серверної аутентифікації і авторизації, а також містить функції перевірки цілісності даних і обмеження приватності;

- розподілений адміністративний сервіс – для кожного хендла в системі можна визначити власного адміністратора (власника). У комбінації з протоколом аутентифікації це дозволяє адміністратору безпечно керувати хендлом через Інтернет.

Принципом даного механізму ідентифікації є використання унікального ідентифікатора для кожного об'єкта IoT. Причому як для вже існуючих пристроїв IoT, в яких використовується ідентифікатор може бути посилений за допомогою DOA, так і нових пристроїв IoT, в яких ДОА ідентифікатор може бути базовим для ідентифікації, простежуваності і боротьби з контрафактом.

У зв'язку з цим, однією з найважливіших проблем є вибір системи ідентифікації для всіх об'єктів, підключених до мережі Інтернет. В якості використання архітектури цифрових об'єктів для ідентифікації речей пропонується безліч різних програмних і апаратних рішень. Для вирішення ряду завдань, поставлених перед етапом повсюдного впровадження архітектури цифрових об'єктів, необхідно проаналізувати методи інтеграції і сумісності унікального DOA ідентифікатора в електронні пристрої IoT.

Як приклади базових технологій передачі даних, що застосовуються для взаємодії пристроїв IoT з мережею Інтернет (як безпосередньо, так і через шлюз) розглянемо технології: WiFi, ZigBee (IEEE 802.15.4) и LoRa (IEEE 802.15.4g). Перелічені технології передачі даних застосовуються в пристроях різного рівня: наприклад, налагодження плати пристроїв IoT як правило мають на борту радіомодуль WiFi (MAC-адресу), а технології Fast і Gigabit Ethernet (сімейство IEEE 802.3 – також використовує MAC-адресу) в мережевих картах пристроїв на базі архітектури x86 або x64, що володіють величезними обчислювальними потужностями. В залежності параметрів

пристроїв IoT, визначається доступний функціонал і методи додавання записів, проте базові методи внесення ідентифікатора в пристрої IoT є однаковими для всіх (рисунок 4.2).

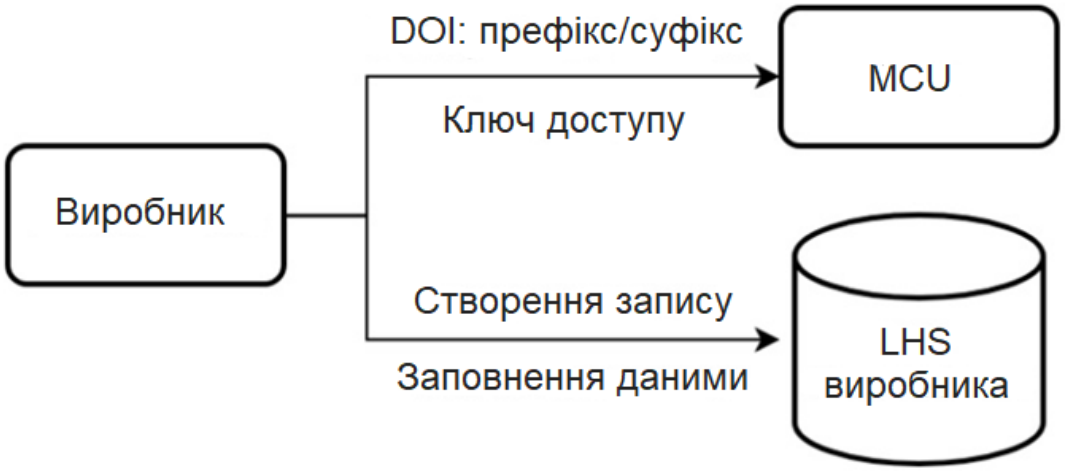

Рисунок 4.2 – Внесення базової інформації в пристрій на мікроконтролері на етапі виробництва

В даному випадку, на етапі виробництва кожен пристрій IoT, який визначається в глобальній системі резолюції, зобов'язаний мати прописаний програмними методами (за аналогією з існуючими ідентифікаторами, такими як MAC або IMEI) цифровий ідентифікатор об'єкта і ключ для доступу до модифікації метаданих ідентифікатора. Вписування цих даних має супроводжуватися створенням відповідних handle-записів в LHS-базах виробника пристрою IoT. Згідно з визначенням, ідентифікатор представляє собою серію цифр, букв і символів або даних в будь-якій іншій формі, яка використовується для ідентифікації абонентів, користувачів, елементів мережі, функцій, об'єктів мережі, що надають послуги / додатки, або інших об'єктів (наприклад, фізичні або логічні предмети).

Отже, наявність у мікроконтролера власної цифрової копії в глобальній системі резолюції обумовлено можливістю створення універсальних методів для ідентифікації пристроїв інтернету речей. В якості подібної інформації,

що зберігається в унікальному для кожного випущеного пристрою домені, може виступати версія доступних протоколів пристрою, прив'язка до інших технологій ідентифікації, супроводжуюча інформація або навіть базові команди доступу для пристрою IoT.

У загальному випадку, ключ доступ і DOI повинні бути доступні для керуючих пристроїв. У разі наявності у керуючого пристрою повноцінної операційної системи, доступ до цих даних здійснюється за допомогою драйвера ОС; якщо в якості керуючого пристрою виступає мікроконтролер, доступ до даних здійснюється через базові команди мікроконтролера.

Прикладом використання (рисунок 4.3) може бути ситуація, коли пристрій 1 за допомогою додатка здійснює запис в доступне для пристрою поле цифрового об'єкта «network_address» актуальну глобальну адресу в мережі TCP / IP. Завдяки цьому можлива взаємодія двох різних пристроїв (1 і 2) без серверів-посередників, які зазвичай надають підтримку у встановленні з'єднання.

Для встановлення з'єднання досить мати DOI пристрою IoT. Зазначений спосіб підходить для складних пристроїв IoT, що містять як мінімум два пристрої на процесорі, прикладом яких є більшість сучасних смартфонів.

Неможливість реалізації криптографічних функцій, необхідних для модифікації даних в системі резолюції, а також відсутність прямих методів доступу в глобальну мережу унеможливлюють реалізацію подібних функцій на простих пристроях (функціонуючих на базі мікроконтролерів або мікрочіпів).

Одночасно з цим, у разі використання мереж для пристроїв IoT в додатках типу «Розумний будинок», що використовують, наприклад, пакет протоколів ZigBee, даний приклад не є реалізованим, тому що прямого доступу до мережі Інтернет, і як наслідок, до системи резолюції у кінцевих пристроїв немає.

Реалізація подібного функціоналу повинна здійснюватися через

програмне забезпечення шлюзів в сукупності з реалізацією необхідного функціоналу в додатках ZigBee. Додатковим функціоналом, необхідним для реалізації на пристроях IoT одночасно з отриманням DOI і унікального ключа є можливість перезапису таких на довільні зі збереженням оригіналу.

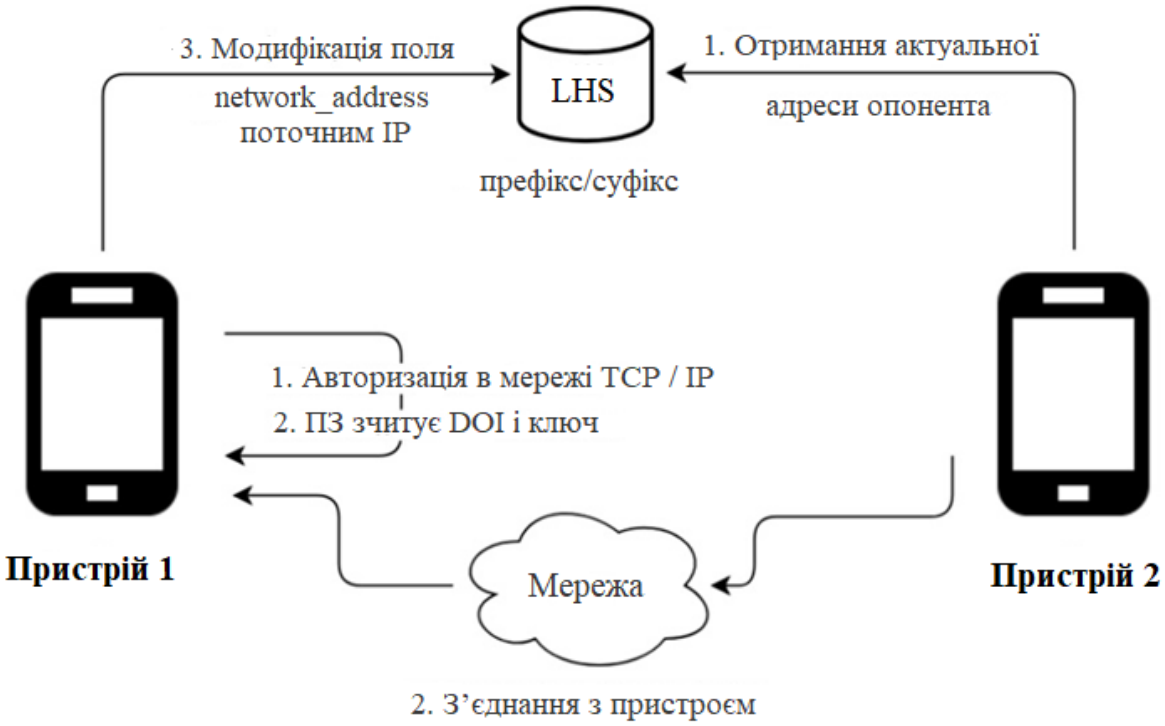

Рисунок 4.3 – Реалізація полів цифрового об'єкта для зберігання мережевої адреси пристрою

Таким чином, виробники пристроїв IoT зобов'язані обмежувати максимальний обсяг даних, що вноситься одним пристроєм IoT в їх домен, припускаючи перепризначення основного (але не вихідного) ідентифікатора цифрового об'єкта і відповідного йому ключа доступу стороннім, з метою збільшення обсягу метаданих і збільшення швидкості доступу до даних. Варто зазначити, що важливо зберігати вихідний DOI, який є одним з можливих доказів автентичності пристроїв, з можливістю його повернення. Даний функціонал може бути використаний в сценаріях боротьби з контрафактом пристроїв інтернету речей.

4.1 Доступ до пристроїв IoT з підтримкою ідентифікації на базі архітектури цифрових об'єктів

Для забезпечення доступності пристроїв IoT їм необхідний стандартний інтерфейс для читання і запису даних, установки параметрів, діагностики специфічних операцій для конкретного пристрою. Дані параметри обов'язково варіюються від пристрою до пристрою тому різноманіття пристроїв IoT дуже широке.

За допомогою фундаментальних компонентів системи глобальної ідентифікації, сховища цифрових об'єктів і сервісу реєстру цифрових об'єктів, архітектура цифрових об'єктів може забезпечити підтримуваний доступ до пристрою IoT. Даний функціонал може бути реалізований за допомогою будь-якого стандартного легковісного протоколу, який використовує поняття глобально одержуваних типів для уточнення доступних операцій. Результатом є можливість прямого доступу до даних або сервісу за допомогою особливого типу запиту на управління або доступу. Не менш важливо, що даний спосіб доступу є виявляємим, а функціонал зрозумілий кожному клієнту в рамках архітектури цифрових об'єктів.

Набір простих дій, заснованих на типах, покликаний забезпечити підтримку всіх типів пристроїв. Переваги такого підходу в тому, що DOA надає гнучку модель даних на базі цифрових об'єктів, що забезпечує базовий, повністю настроюваний і розширюваний підхід для забезпечення доступу до даних будь-якого пристрою IoT. DOA підтримує доступ до пристрою IoT за допомогою будь-якого протоколу, що дозволяє виконувати будь-які пристрій-залежні операції.

Наприклад, пристрій IoT дає можливість виконання особливих дій для установки точних калібрувальних параметрів, конфігурування пристрою, або додавання запису у внутрішню власну базу даних.

Виробник може визначити подібні дії шляхом створення нового цифрового об'єкта для представлення інформації про пристрій, з унікальним

ідентифікатором і пов'язаним описом дії в супровідній інформації. Коли клієнт здійснює запит до пристрою IoT за допомогою базового протоколу, з метою отримання списку можливих дій, які виконуються пристроєм, пристрій IoT повертає той особливий тип дії, властивий для даного виробника.

За допомогою системи типів, що є притаманною для архітектури цифрових об'єктів, клієнт може визначити тип операцій, дізнатися, чи є дані дії корисними для використання. Дана притаманна розширюваність протоколів може бути використана будь-якими виробниками пристроїв IoT для розробки нових типів дій, при цьому здійснюючи підтримку старих типів дій.

4.2 Аспекти мережевої взаємодії

Сервіс глобальної ідентифікації дозволить призначати глобальний ідентифікатор будь-якому цифровому об'єкту. Даний сервіс надає протокол резолюції і адміністрування, призначений для визначення пов'язаної з цифровим об'єктом допоміжної інформації: місце зберігання, походження інформації, з можливістю вилучення і управління з дотриманням необхідних заходів безпеки.

Сервіс ідентифікації повинен бути розподіленою системою з вбудованими механізмами захисту для забезпечення цілісності сервісу, його безвідмовності, цілісності даних, що зберігаються.

Обов'язковою є також аутентифікація і конфіденційність операцій з збереженими даними, наявність виборчого управління доступом для будь-яких метаданих, пов'язаних з ідентифікатором.

Набір розподілених сервісів для зберігання цифрових об'єктів сприяє безпечному зберіганню, доступу і розповсюдження об'єктів з використанням їх ідентифікаторів.

Саме сховище є цифровим об'єктом, яке може зберігати в собі інші

об'єкти (що не є обов'язковим). Цифровий об'єкт може виконувати певний набір дій, включаючи здійснення доступу до інших цифрових об'єктів, створення нових цифрових об'єктів і ін. Місце цифрових об'єктів може представляти із себе набір пристроїв IoT, які при цьому є також цифровими об'єктами.

Цифровий об'єкт може мати безліч атрибутів, пов'язаних з реальним об'єктом. Частина атрибутів може описувати природу пристрою IoT. Зокрема, об'єкт може володіти керуючими атрибутами, які пов'язані з програмним забезпеченням, надаючи пряму взаємодію з функціями пристрою IoT, наприклад, включення або виключення системи, отримання показань температурного сенсора на пристрої.

Крім цього, цифровий об'єкт може також мати атрибути, що визначають доступність основних атрибутів пристроїв, таким чином визначаючи, хто може взаємодіяти з пристроєм IoT за допомогою інтерфейсу, описаного в атрибутах об'єкта.

На рисунку 4.4 представлена схема взаємодії пристроїв IoT, що підключаються до мережі зв'язку з використанням різних технологій передачі даних.

Структура цифрового об'єкта може бути сформована у вигляді цифрового уявлення фізичного пристрою IoT. Система компонентів, а саме реєстр, має можливості для визначення способів знаходження та доступу до подібних сутностей. Критерій сумісності в термінах IoT має на увазі наявність API, щоб цифрові об'єкти могли взаємодіяти з пристроями, до яких вони прив'язані.

Даний підхід може бути використаний для досягнення конкретних засобів управління доступом для зручності кожного сховища. З іншого боку, сховище може надавати доступ до даних, що генеруються окремим пристроєм IoT. Архітектура цифрових об'єктів не обмежує кількість можливих сховищ.

Набір сервісів реєстрів цифрових об'єктів в межах однієї області

(входить до складу MPA) дозволяє виявляти будь-який цифровий об'єкт. Реєстр цифрових об'єктів може також надавати можливість пошуку за метаданими або простими даними в цифровому об'єкті.

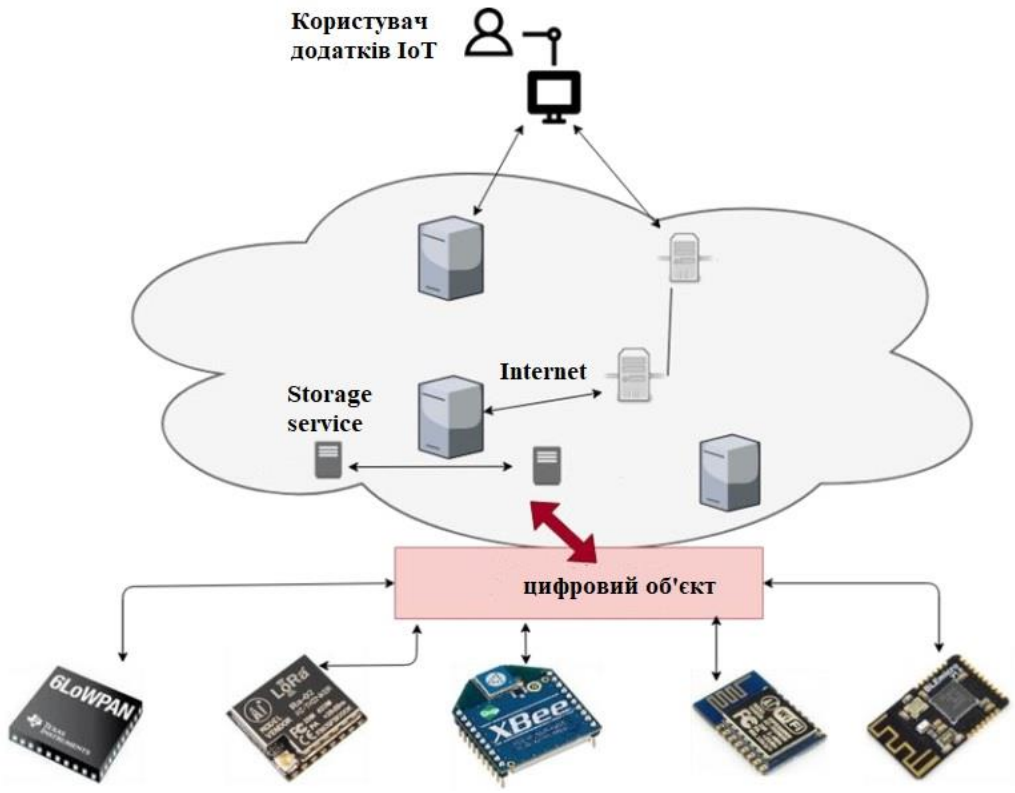

Рисунок 4.4 – Схема взаємодії пристроїв IoT і компонентів архітектури цифрових об'єктів

Використання реєстру дозволяє виявляти цифрові об'єкти за різними критеріями, наприклад:

- пошук по різним типам записів метаданих цифрових об'єктів в межах різних сервісів-реєстрів;

- пошук по різних рівнях мережевої взаємодії в межах різних сервісів-реєстрів;

- пошук по різним видам сервісів по управлінню даними;

- пошук по різним типам безпеки і системам контролю доступу.

Політика доступу, що включає в себе аутентифікацію і авторизацію

клієнтських запитів, що застосовується на множині MPA, повинна бути явно визначена.

4.3 Метод ідентифікації пристроїв IoT на базі архітектури цифрових об'єктів

Як було описано вище, система резолюцій складається з двох типів реєстрів – GHR і LHR. Нехай група реєстрів GHR визначається символом $G_j, j = 1,2,.....,N$, де N – загальне число реєстрів GHR в системі. Кожен реєстр GHR об'єднує і контролює певний набір локальних реєстрів. Набір локальних реєстрів, приєднаних до j-го GHR, позначається символом $L_i^j i, j = 1,2,.....,M_j$ де M_j – загальне число LHR, приєднаних до j-го GHR. Передані пакети прибувають на сервер з певною частотою, що відповідає пуассонівському процесу, формуючи поодиноку чергу на контролері. Така система може бути змодельована на основі багатоканальної моделі масового обслуговування (M/M/s).

Тоді середній час відповіді T_j реєстру GHR дорівнює сумі часу в черзі і часу обробки, і може бути обчислено як функція частоти надходження λ_i запитів і частоти обслуговування μ:

$$T_j = \frac{f(S, \frac{\lambda_j}{\mu})}{s\mu_j - \lambda_j} + \frac{1}{\mu} \qquad (4.1)$$

Функція γ показує використання системи, що відображає також її стабільність. Система стабільно розподілена тільки якщо показник використання системи γ менше одиниці. Дана інформація може бути коректно інтерпретована за допомогою діаграми станів багатоканальної моделі M/M/s. У разі, коли число заявок в черзі більше, ніж на сервері

контролера, обробка буде відбуватися з тією ж частотою μ, при цьому контролер буде гранично заповнений.

Розглядаючи відмінності основних компонентів системи, варто відзначити об'єднання Global Handle Register і Local Handle Register в один об'єкт для здійснення випробувань. Учасникам дослідження був наданий доступ до тестової зони DOA з префіксом “11.test”, що дозволяє розмістити власні ідентифікатори в існуючій системі Digital Object Architecture. У перспективі, це дає можливість оцінити безліч характеристик розроблюваної системи на прикладному рівні.

Рівень верифікації був представлений програмно-апаратним комплексом з набором мережевих інтерфейсів, що дозволяють підключати безліч різних пристроїв, як шляхом безпосередньої фізичної взаємодії (технології NFC), так і за допомогою мережевої взаємодії (BLE, WiFi). Кінцевий пристрій може являти собою як пристрій інтернету речей, так і звичайний об'єкт, верифікація якого необхідна в будь-якому контексті.

Процес верифікації пристрою з ідентифікатором DOA відбувається поетапно:

- за допомогою одного з доступних інтерфейсів виробляється звернення до пристрою верифікації, яке включає в себе передачу масиву даних, що містить цифровий ідентифікатор об'єкта, а також дані, за якими безпосередньо відбувається перевірка істинності об'єкта – MAC-адреса, BLE адреса, дата продажу продукту, унікальний номер продукту та ін.;

- пристрій верифікації визначає необхідний сервер для звернення, відправляє запит по заданому ідентифікатору об'єкта;

- handle-сервер відповідає на запит JSON-масивом, що містить необхідні поля, в тому числі поля, що відповідають за перевірку об'єкта на відповідність;

- пристрій верифікації порівнює отримані дані по заданим полям,

видає результат перевірки (як на засіб виведення інформації, так і безпосередньо на верифікований пристрій).

Таким чином, пристрій проходить перевірку через строго задані сервера DOA (рисунок 4.5), захищені від прямого доступу для звичайних користувачів, не виказуючи при цьому дані по запитуваному ідентифікатору.

Данный подход ограничивает возможные сценарии подделки устройств с цифровым идентификатором, одновременно разгружая конечное устройство.

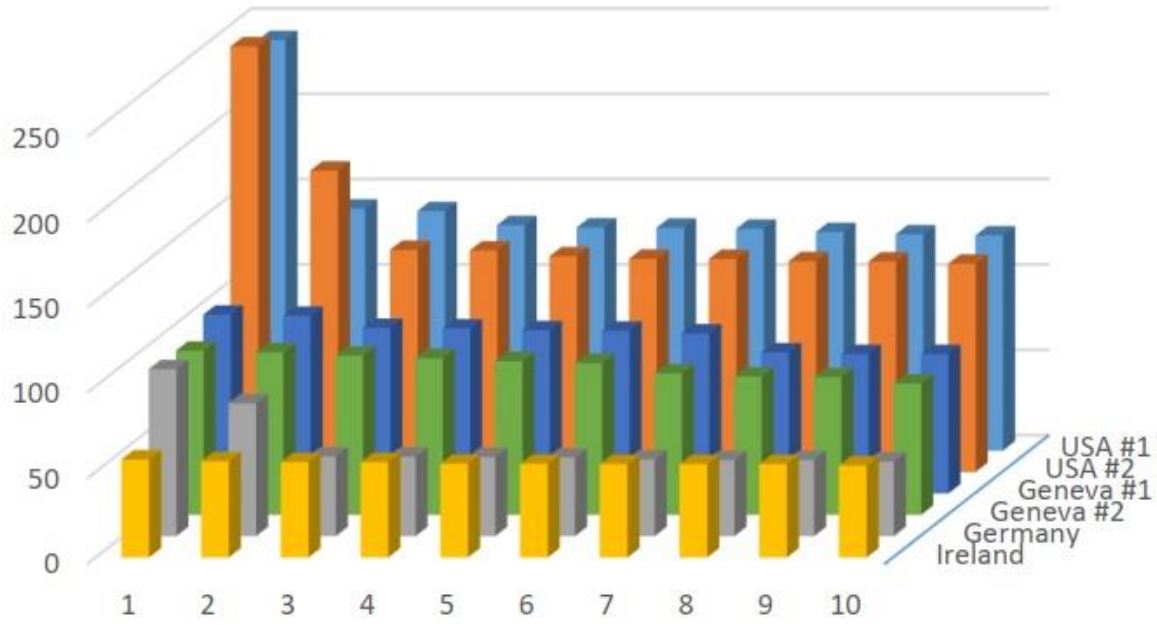

Рисунок 4.5 – Графік мережевої затримки при відправці запиту в різні країни

Отримана система в стаціонарному виконанні (у вигляді стенду) також дозволяє наочно продемонструвати швидкість процесу ідентифікації, маршрут прямування службового трафіку та інші параметри.

Введення в традиційну схему пристрою перевірки дозволить визначити

середній час доступу системи до DOA-сервера і надасть статус перевірки.

Доступ до перевірочного пристрою з використанням спеціальних технологій на кшталт як NFC або BLE, створює додаткові затримки на інтерфейсах, але це не цільовий сценарій для даного дослідження.

Затримки вимірювалися в двох випадках:

- використання системи проксі-серверів CNRI, набір веб-серверів, які розуміють протокол обробки. Система складається з чотирьох різних веб-серверів, розміщених в трьох різних географічних зонах;
- використання основного сервера GHR, розміщеного в Женеві.

У таблиці 4.1 міститься час затримки для кожного сервера і середня затримка на основі десяти експериментів. Кожен запит виконувався з використанням REST API, що дозволяє обробляти запити в форматі JSON. Тимчасові інтервали були отримані за допомогою програмного забезпечення для захвату пакетів Wireshark.

Таблиця 4.1 – Результати вимірювання затримки з використанням різних handle – серверів

Місце-знаходження	Затримка, ms								
	1	2	3	4	5	6	7	8	Серед-ня
США #1	140,2	240,4	141,7	132,0	130,6	126,6	126,0	129,9	142,6
США #2	249,2	130,0	123,2	121,9	176,4	126,2	123,4	124,7	142,9
Німеччина	97,6	43,6	44,4	77,6	46,4	45,9	46,2	46,5	53,7
Ірландія	53,8	57,3	54,6	54,6	54,7	54,8	55,7	55,7	55,2
Женева #1	81,5	82,5	95,2	103,9	93,5	95,4	81,5	104,5	93,1
Женева #2	80,4	93,0	91,5	88,7	94,9	95,9	89,8	76,7	87,4

Як видно з таблиці 4.1, оптимальне значення затримки спостерігається

при обміні даними з сервером, розташованим в Німеччині, а найгірше значення – з сервером, розташованим в США. Грунтуючись на цих значеннях, ми можемо зробити висновок, що для мінімізації затримки необхідно оптимізувати маршрути для звернень до серверів GHR.

ВИСНОВКИ

В результаті виконання магістерської атестаційної роботи було проаналізовано склад факторів, що впливають на ідентифікацію IoT. Визначено узагальнені основні особливості ідентифікації для інтернету речей. Запропоновано модель системи резолюції ідентифікаторів цифрових об'єктів як системи масового обслуговування, на базі якої виконаний оптимізаційний експеримент і отримана конфігурація системи резолюції, що дозволяє скоротити час на дозвіл ідентифікатора пристрою. Розроблено метод ідентифікації пристроїв IoT на базі архітектури цифрових об'єктів. Система резолюцій ідентифікаторів DOA була представлена у вигляді СМО.

Розроблено імітаційну модель, яка з заданим рівнем абстракції відтворює обмін даними між компонентами DOA. Проведені експерименти з імітаційної моделлю показали, що дозвіл ідентифікатора в системі відбувається набагато швидше на базі запропонованого методу звернень до MPA. Приріст швидкості в 15 разів досягається на максимальній інтенсивності навантаження сервера. Розроблено математичну модель системи резолюцій. На базі отриманої формули Ерланга можна зробити чисельний розрахунок середнього навантаження Lj на реєстрах GHR. Проведено натурний експеримент по дослідженню затримки при передачі даних в системі «архітектура цифрових об'єктів». Аналіз результатів натурного експерименту показав, що оптимальне значення затримки спостерігається при обміні даними з сервером, розташованим в Німеччині, а найгірше значення – з сервером, розташованим в США.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Токарев В.В. Разработка алгоритма мультиагентного управления группой мобильных «s-bot» / В. Н. Ткачев, В. В. Токарев, Г. И. Чурюмов // Реєстрація, зберігання і обробка даних. - 2019, Т. 21, № 1 – С.46-56.

2. Токарев В.В. Надширокосмугові технології в системах управління мобільними об’єктами / О. А. Серков, П. Є. Пустовойтов, І. В. Яковенко, Б. О. Лазуренко, Г. І. Чурюмов, В. В. Токарєв, Ванг Наннан // Сучасні інформаційні системи. - 2019, Т.3, №2 – С.22-27.

3. Volodymyr Tokariev. Ultra Wideband Signals in Control Systems of Unmanned Aerial Vehicles / Aleksandr Serkov, Valeri Kravets, Igor Yakovenko, Gennady Churyumov, Wang Nannan // The 10h IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2019 5-7 June, 2019, Leeds, United Kingdom. - Pp.26 - 29.

4. Tokariev Volodymyr. Problem of self-organization of s-bot group movement in unorganized physical environment / Churymov Gennadiy, Tokariev Volodymyr, Tkachov Vitalii // Комп’ютерні та інформаційні системи і технології: тези доповідей третьої міжн. наук. - техн. конф. 23 - 24 квітня 2019 р. - Харків, Україна. - С.16-17.

5. 5.Volodymyr Tokariev. Method for Ensuring Survivability of Flying Ad-hoc Network Based on Structural and Functional Reconfiguration / Genadiy Churyumov, Vitalii Tkachov, Volodymyr Tokariev, Vladyslav Diachenko // Selected Papers of the XVIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2018) / Kyiv, Ukraine, November 27, 2018. – Pp. 64-76.

6. Volodymyr Tokariev. Method of Data Collection in Wireless Sensor Networks Using Flying Ad Hoc Network / Vitalii Tkachov, Volodymyr Tokariev, Yana Dukh, Vadym Volotka // 2018 5th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology, October 9-

12, 2018 Kharkiv, Ukraine. – Pp.197 - 201.

7. Tokariev,V. Scenario of Interaction of the Mobile Technical Objects in the Process of Transmission of Data Streams in Conditions of Impacting the Powerful Electromagnetic Field / G. Churyumov, V. Tokarev, V. Tkachov, S. Partyka // 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP). – 21-25 Aug. 2018. – Pp. 183-186.

8. Токарев В.В. Темпоральная модель адаптации интегрированной информационной системы путем реконфигурации логической структуры / О.Г. Лебедев, В.Н. Ткачев, В.В. Токарев, Г.И. Чурюмов // Комп'ютерні та інформаційні системи і технології: тези доповідей другої міжн. наук. - техн. конф. 18 - 19 квітня 2018 р. - Харків, Україна. - С.6-7.

9. Tokarev V.V. SHORTEST PATH BRIDGING METHOD FOR THE GROUP OF MOBILE TECHNICAL OBJECTS/ V.M. Tkachov, V.V. Tokarev, G.I. CHURYUMOV//СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ: матеріали VIII - межд. наук. - техн. конф., 26 - 27 квітня 2018 р. - Харків, 2018р. - С.18.

10. Volodymyr V. Tokarev. Provision of Survivability of Reconfigurable Mobile System on Exposure to High-Power Electromagnetic Radiation / Igor V. Ruban, Genadiy I. Churyumov, Volodymyr V. Tokarev, Vitaliy M. Tkachov // Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017). – CEUR Workshop Processing. – Kyiv, Ukraine, November 30, 2017. – Pp. 105-111.

11. СТВОРЕННЯ НАУКОВО-МЕТОДИЧНИХ ОСНОВ ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ МЕРЕЖЕВИХ СИСТЕМ ОБМІНУ ІНФОРМАЦІЄЮ В УМОВАХ ЗОВНІШНЬОГО ВПЛИВУ ПОТУЖНОГО НВЧ ВИПРОМІНЮВАННЯ // Г.И. Чурюмов, В.В. Токарев, И.В. Рубан, В.Н. Ткачев и др. // ЗВІТ ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ за договором від 20.09.2017 р. № Ф76/109-2017 (заключний). № держреєстрації 0117U003916. ХИРЭ. - 116с.

12. Спосіб передачі цифрових даних мультикоптерною системою між сегментами розподіленої сенсорної мережі та базовою станцією [Текст] : пат. 118921 Україна: МПК 2017.01, H04W 64/00, H04W 84/18 (2009.01), G06F 17/40 (2006.01) / Ткачов В.М., Токарєв В.В., заявник та патентовласник Харківський національний університет радіоелектроніки. – u2017 04085; заяв. 24.04.2017; опубл. 28.08.2017, бюл. № 16. – 2017. – 5 с.

13. Токарев В.В. Мобильная подсистема «Мультикоптер-сенсорная сеть» в компьютерной системе хранения BIG DATA / В.О. Радченко, Д.А. Руденко, В.Н. Ткачов, В.В. Токарев // Системи управління, навігації та зв'язку - 2017. - №4(44). – С.102-105.

14. Токарев В.В. Проблема передачі даних типу BIG DATA у мобільній системі «МУЛЬТИКОПТЕР - СЕНСОРНА МЕРЕЖА» / В.М. Ткачов, В.В. Токарев, В.О. Радченко, В.О. Лебедєв // Системи управління, навігації та зв'язку - 2017. - №2(42). – С.154-157.