УДК. 004.72 DOI: 10.31673/2786-8362.2023.010606

Каргаполов Ю.В., Вишнівський В.В., д.т.н.,
Єрмоленко В.О., Чичкарьов Є.А., д.т.н.

ПРОБЛЕМНІ ПИТАННЯ КЕРУВАННЯ ІДЕНТИФІКАЦІЄЮ ЦИФРОВИХ ОБ'ЄКТІВ МУЛЬТИСЕРВІСНИХ СИСТЕМ

Kargapolov Yu.V., Vyshnivskyi V.V., Yermolenko V.O., Chychkarov E.A. Problem issues of identification management of digital objects of multiservice systems. The paper considers the issues of access to the ecosystem of services, obtaining and providing services, which can be both internal and external in relation to the information system in which the digital object is located. Today, the management of relationships between digital objects and services is carried out not only due to the functionality provided by the information system, but also, in particular, due to the management of the identification of digital objects and services.

As a digital object, not only the object that wants to receive or provide services, but also the service itself is considered. Therefore, identity management is considered in relation to two interacting objects.

The analysis of digital object identification management was carried out based on the following circumstances. Identification of the same digital objects can be expressed in different sign and meaning systems. Therefore, it is necessary to update and maintain many identifiers within one ecosystem of services and be able to manage them.

Identifiers can be divided into "stupid" (limited), which cannot perform anything except the function of linking a digital object to a strictly limited set of operations within the information system, regardless of the conditions in which it is located, and "smart", which can provide an opportunity to respond to circumstances and the possibility of implementing a flexible scenario selection that can be updated according to the situation. "Smart" identifiers, unlike "stupid" ones, have properties that allow them to respond to circumstances, and therefore it is necessary to be able to manage such properties of identifiers.

The principles of a new architecture for the design of computer systems are proposed, which allow flexible management of digital objects, their properties, identification of digital objects, properties of identifiers depending on the circumstances of the time, place and situation in which the digital objects are located.

The new architecture makes it possible to integrate new entities into information systems without significant modernizations associated with changes in source and object code, information schemes of systems, modernization of data structures, which lead to the need for mandatory restructuring of database tables and database table management procedures data.

Keywords: architecture, computer system, identification, service, service, digital object

Каргаполов Ю.В., Вишнівський В.В., Єрмоленко В.О., Чичкарьов Є.А. Проблемні питання керування ідентифікацією цифрових об'єктів мультисервісних систем. В роботі розглянуті питання доступу до екосистеми сервісів, отримання та надання послуг, які можуть бути як внутрішніми, так і зовнішніми по відношенню до інформаційної системи, в якій знаходиться цифровий об'єкт. На сьогоднішній день управління взаємозв'язками між цифровими об'єктами і сервісами здійснюється не тільки за рахунок функціональності, що забезпечується інформаційною системою, але зокрема й за рахунок управління ідентифікацією цифрових об'єктів і сервісів.

В якості цифрового об'єкта розглянуто не тільки той об'єкт, який хоче отримати або надати послуги, а й сам сервіс. Тому управління ідентифікацією розглянуто щодо двох об'єктів, які вступають у взаємодію.

Аналіз управління ідентифікацією цифрового об'єкта проведено виходячи з наступних обставин. Ідентифікація одних і тих самих цифрових об'єктів може виражатися у різних знакових і смислових системах. Тому у межах однієї екосистеми сервісів необхідно актуалізувати і підтримувати безліч ідентифікаторів та вміти керувати ними.

Ідентифікатори можна розділити на «дурні» (обмежені), які нічого не можуть виконувати крім функції прив'язки цифрового об'єкта до строго обмеженого в рамках інформаційної системи набору операцій незалежно від умов, в яких він знаходиться, та «розумні», які можуть надавати можливість реагувати на обставини та можливість реалізації гнучкого вибору сценарію, що може актуалізуватися за ситуацією. «Розумні» ідентифікатори на відміну від «дурних» мають властивості, які дозволяють їм реагувати на обставини, а отже, необхідно вміти керувати такими властивостями ідентифікаторів.

Запропоновано принципи нової архітектури проектування комп'ютерних систем, що дозволяють гнучке управління цифровими об'єктами, їх властивостями, ідентифікацією цифрових об'єктів, властивостями ідентифікаторів залежно від обставин часу, місця та ситуації, у яких знаходяться цифрові об'єкти.

Нова архітектура дає можливість інтеграції нових сутностей у інформаційні системи без значних модернізацій, пов'язаних із зміною вихідного та об'єктного коду, інформаційних схем систем, модернізації структур даних, що призводять до необхідності обов'язкової реструктуризації таблиць баз даних та процедур управління таблицями баз даних.

Ключові слова: архітектура, комп'ютерна система, ідентифікація, сервіс, послуга, цифровий об'єкт

Вступ

Метою функціонування цифрових об'єктів (далі - ЦО) в інформаційній системі є доступ до екосистеми сервісів, отримання та надання послуг, які можуть бути як внутрішніми, так і зовнішніми по відношенню до інформаційної системи, в якій знаходиться ЦО. Управління взаємозв'язками між ЦО і сервісами здійснюється не тільки за рахунок функціональності що забезпечується інформаційною системою, але зокрема й за рахунок управління ідентифікацією ЦО і сервісів.

Під цифровим об'єктом ми розумітимемо не тільки той об'єкт, який хоче отримати або надати послуги, а й сам сервіс. Таким чином, управління ідентифікацією це процес, який має розглядатися щодо двох об'єктів, які вступають у взаємодію.

Тому необхідно провести аналіз питань управління ідентифікацією ЦО, які є проблемними через наступні обставини.

По-перше, ідентифікація одних і тих самих ЦО може виражатися у різних знакових і смислових системах. Це означає, що для будь-якого ЦО у межах однієї екосистеми сервісів необхідно актуалізувати і підтримувати безліч ідентифікаторів. З іншого боку, застосування ідентифікаторів залежить від обставин, в яких ЦО знаходиться або від яких залежить в цілому, або в даний момент, а також впливає на ухвалення рішення, оскільки не кожен ідентифікатор може вибрати необхідну дію. Це означає, що для будь-якого ЦО в рамках однієї екосистеми сервісів необхідно актуалізувати та підтримувати безліч ідентифікаторів та вміти керувати ними.

Сучасні інструментальні рішення для таких завдань у загальному вигляді дозволяють формувати лише статичні зв'язки між ЦО та спрямовані на строго певний порядок взаємодії між ними. Вихід за межі попередньо визначеної структури взаємодії ЦО з сервісами та/або іншими ЦО призводить до необхідності перебудови інформаційних схем і структури зберігання даних у інформаційних системах.

Наприклад, якщо система була орієнтована на обслуговування ЦО, для яких ідентифікаторами були VIN-коди транспортних засобів, а тепер необхідно, щоб вона додатково обслуговувала транзакції з надання сервісів для нових класів ЦО, що асоціюються з уже існуючими або раніше не існували в системі, які будуть використовувати ідентифікатори у вигляді MSISDN, при цьому пов'язуючи інформаційні потоки даних для обох типів класів ЦО в єдине ціле, актуальні рішення передбачають модифікацію існуючих таблиць бази даних інформаційної системи, створення і введення нових таблиць в базу даних системи з переіндексацією взаємозв'язків сутностей і наступним налагодженням нових процесів обробки інформації.

Зрозуміло, що такі дії виведуть процес експлуатації із нормального режиму та, можливо, вимагатимуть зміни організаційної структури підтримки системи.

По-друге, ідентифікатори можна розділити на «дурні» (обмежені), які нічого не можуть виконувати крім функції прив'язки ЦО до строго обмеженого в рамках інформаційної системи набору операцій незалежно від умов, в яких знаходиться ЦО, та «розумні», які можуть надавати можливість реагувати на обставини, в яких знаходиться ЦО та можливість реалізації гнучкого вибору сценарію, що може актуалізуватися за ситуацією. «Розумні» ідентифікатори на відміну від «дурних» мають властивості, які дозволяють їм реагувати на обставини, а отже,

необхідно вміти керувати такими властивостями ідентифікаторів, що також є погано вирішеним завданням на сьогоднішній день.

По-третє, існуючі підходи до управління ідентифікацією є рішеннями, орієнтованими на забезпечення безпечного доступу ЦО до екосистеми сервісів.

У цьому пункті необхідно зробити ремарку щодо використання термінології. Управління ідентифікацією описується терміном «Identity Management», тобто управління ідентичністю. Цей термін є загальновизнаним та відповідний підхід описаний у стандартах та звітах МСЕ [3], ETSI [4, 5], RFC [6 - 8], 3GPP [9, 10], та інших інституцій. Визначено, що «Identity Management» має на меті управління надійними зразками ознак, подій, тенденцій чи інших спостережуваних характеристик об'єкта. Сам термін визначається як набір функцій та можливостей (наприклад, адміністрування, управління та технічного обслуговування, виявлення, обміну повідомленнями, зіставлення та прив'язуванням, забезпеченням реалізації політики, автентифікації та авторизації, тобто затвердження прав доступу), що використовуються для: гарантування інформації, що підтверджує ідентичність (наприклад, ідентифікаторів, повноважень, атрибутів); гарантування ідентичності об'єкта та забезпечення комерційних додатків та додатків безпеки. При цьому опис функціоналу «Identity Management» належить до галузі безпеки в частині операцій автентифікації та авторизації прав доступу цифрових об'єктів в рамках системи.

Аналіз запропонованого функціоналу Identity Management не дозволяє говорити про наявність інструментарію, який дає можливість керувати ідентифікацією ЦО в процесі отримання безпосередньо послуг. У частині доступу до можливості отримання та надання послуг в екосистемі сервісів – так, у частині управління яким чином ЦО може визначити логіку отримання та надання послуг та зміни умов їх отримання залежно від обставин, що виникають – ні.

Тому в статті необхідно провести дослідження не про здатність за рахунок засобів ідентифікації проводити операції аутентифікації та авторизації доступу до сервісів екосистеми, а здатність цифрових об'єктів до вибору необхідного сервісу та його показників за умовами, які визначають необхідність обслуговування цифрового об'єкта в поточних обставинах.

У Рекомендації МСЕ-Т Y.4403 [1] наводиться загальна модель функціональної архітектури (overall functional architecture model), яка містить опис двох страт - сервісної (Service Stratum) та транспортної (Transport Stratum), які у свою чергу містять опис управління:

1) послугами та доставки контенту (service control and content delivery functions),
2) підтримкою додатків та сервісів (application and service support functions) та
3) мережевим транспортом (transport control functions).

Управління у межах зазначених страт пов'язано з функціоналом:

1) провайдерів сервісів (Functions from other Service Providers) через інтерфейс сервісного вузла (Service node interface),
2) операторів електронних комунікацій (Functions from other networks) через міжмережевий інтерфейс (Network-to-network interface),
3) користувачів сервісів та послуг електронних комунікацій (End-User functions) через користувальницький мережевий інтерфейс (User network interface),
4) управління ідентичності ЦО (IdM Functions).

Детальне розкриття функцій керування ідентичністю ЦО (Identity Management Functions), що не стосується завдань автентифікації та авторизації доступу у Рекомендації МСЕ-Т Y.4403, не розглядається. Також відсутній детальний опис функцій вибору ЦО необхідного сервісу та його характеристик за поточними умовами у Рекомендації МСЕ-Т Y.4000 [2], яка описує еталонну модель IoT. У Рекомендації МСЕ-Т Y.4000 наводиться деталізація щодо функцій керування провайдерів сервісами, керування операторів електронних комунікацій та керування користувачів. Еталонна модель передбачає 4 рівні (див. рисунок 1):

1) пристроїв (Device level),
2) мережевий (Network level),
3) серверний (Service support and application support level),
4) застосувань (Application level).

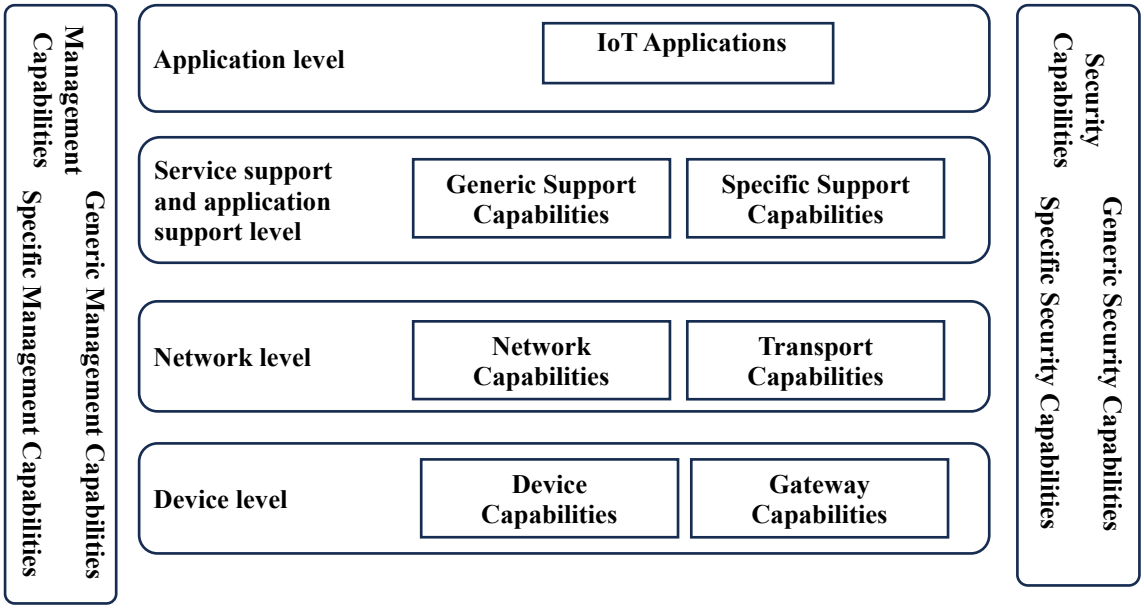

Рис. 1. Еталонна модель IoT

Ні для одного з рівнів не визначено яким чином може бути реалізована функція управління ідентичності у виді, що нас цікавить, незважаючи на те, на будь-якому з чотирьох рівнів відбувається взаємодія безлічі різних за своєю природою ЦО, які в силу своєї різнорідності мають різні властивості і системи ідентифікації. Єдине посилання в цікавому для нас аспекті наведено щодо забезпечення безпеки, тобто операцій аутентифікації та авторизації прав доступу в частині опису загальних та спеціалізованих можливостей безпеки (Generic and Specific Security Capabilities).

Постановка наукового завдання. Основним завданням управління ідентифікацією цифрових об'єктів мультисервісних систем є створення середовища, що дозволяє вибудовувати багатовимірні та багатофакторні зв'язки між цифровими об'єктами, які використовують різні сервіси, методи, протоколи, типи та структури даних, системи ідентифікації тощо. Актуальність розв'язання таких завдань надає розвиток мультисервісних конвергентних систем Інтернету речей, комп’ютерних систем, тобто є практикою розвитку електронних комунікацій. З іншого боку, поняття «Identity Management» надане в документах MCE, IETF, ETSI та ін. сфокусоване на вирішенні завдань управління аутентифікацією та авторизацією прав доступу цифрових об'єктів, об'єктивно не пропонує шляхів для вирішення означеного завдання.

Еталонна модель, що передбачає чотири рівні розгляду управління процесами функціонування систем та надання послуг, потребує розширення так як. не містить відповіді на питання – як управління ідентифікацією пов'язані з іншими робочими процесами мультисервісних систем складних цифрових об'єктів у багатофункціональному мультисервісному середовищі. Виходячи з цього, дослідження питань покращення управління ідентифікацією цифрових об'єктів мультисервісних систем є актуальними.

Таким чином, в даній статті вирішується **наукове завдання** дослідження нових принципів побудови як власне підсистеми ідентифікації в рамках мультисервісних систем, так і новий підхід проектування архітектури послуг у мультисервісному середовищі.

Метою роботи є підвищення ефективності управління ідентифікацією цифрових об'єктів мультисервісних систем.

Виклад основного матеріалу дослідження.

Розглянемо процес отримання та надання послуг у рамках будь-якого сервісу. Насамперед відзначимо, будь-який аналізований сервіс є складовою екосистеми сервісів, тобто мультисервісної системи, доступ до послуг якої хоче отримати ЦО.

Можна розділити процес отримання та надання послуг у рамках сервісу на два етапи:

1) етап отримання доступу до сервісу;

2) етап управління процесом отримання та надання послуг.

Відповідно до положень стандартів [3, 4, 5, 6, 7, 8, 9] на етапі отримання доступу до сервісу визначальним є здатність управління ідентичністю (Identity Management) ЦО. Етап отримання доступу до сервісу досить докладно описаний у наведених вище стандартах, а також у ряді стандартів і кращих поточних практиках інших інституцій, що базуються на положеннях Рекомендацій МСЕ-Т.

На етапі керування процесом отримання та надання послуг ключовою є здатність керування ідентифікацією ЦО, предмет якої не описаний у стандартах.

Тому розглянемо управління ідентифікацією на етапі управління процесом отримання та надання послуг.

Вище було зазначено, що ідентифікатори можуть бути «дурними» та «розумними». Інтерес представляє предмет управління «розумними» ідентифікаторами, оскільки управління «дурними» буде окремим випадком.

Відмінною особливістю «розумного» ідентифікатора є закладена в його структуру здатність реагувати на обставини, що пов’язані з умовами отримання та надання послуг. Прикладами таких ідентифікаторів можуть бути доменне ім’я або URI, що містить облікові дані (credentials).

Наявність у ідентифікатора структури та властивостей, що дозволяють адаптуватися до ЦО при отриманні послуг під поточні обставини, змушує розділити завдання управління ідентифікацією на:

1) управління властивостями ідентифікаторів,

2) управління процесом ідентифікації.

Залишається відкритим питання, що розуміти під «поточними обставинами», які можуть визначати особливості які виникають при отриманні послуг конкретним споживачем.

У Рекомендації МСЕ-Т Y.4000 такими обставинами визначаються можливості:

1) зв’язки в будь-який час (any time communication),

2) зв’язки в будь-якому місці (any place communication),

3) зв’язки із будь-якою річчю (any thing communication).

Логічно припустити, що будь-який ЦО знаходиться в обставинах, що визначаються його місцезнаходженням (place communication) та часом доби (time communication). Наприклад, при знаходженні в тому самому місці на трасі, у світлий час доби власнику транспортного засобу може знадобитися одна послуга, а вночі ця послуга може бути вже іншою. Аналогічно можна припустити, що у один і той же час залежно від місцезнаходження туриста у подорожі можуть знадобитися зовсім різні послуги.

Однак, щодо обставин зв’язку з будь-якою річчю (thing communication), які специфіковані в Рекомендації МСЕ-Т Y.4000 як можливості взаємозв’язку з будь-якими фізичними сутностями, то вони не дозволяють визначати умови, у яких за рівних обставин часу і місця ЦО можна буде змінити вимоги щодо отримання та надання послуг. Це пояснюється тим, що можливість взаємозв’язку фізичних сутностей сама по собі не може визначати особливості отримання цими сутностями послуг (див. рисунок 2).

Взаємозв’язок цифрових об’єктів визначає вибір послуг і характеру послуг, але як не обставини, в яких знаходиться ЦО, а як фактор зведення кількох ЦО в систему.

Третім фактором, що визначає вибір сервісу поряд з факторами часу та місця, є обставини ситуації, в якій знаходиться ЦО.

Пропонується під "поточними обставинами" або під умовами отримання сервісу "тут і зараз" для ЦО, що можуть визначати які особливості виникають при отриманні послуг

цифровим об’єктом розглядати триплет обставин {"часу", "місця", "ситуації"}, в яких знаходиться ЦО (рисунок 3).

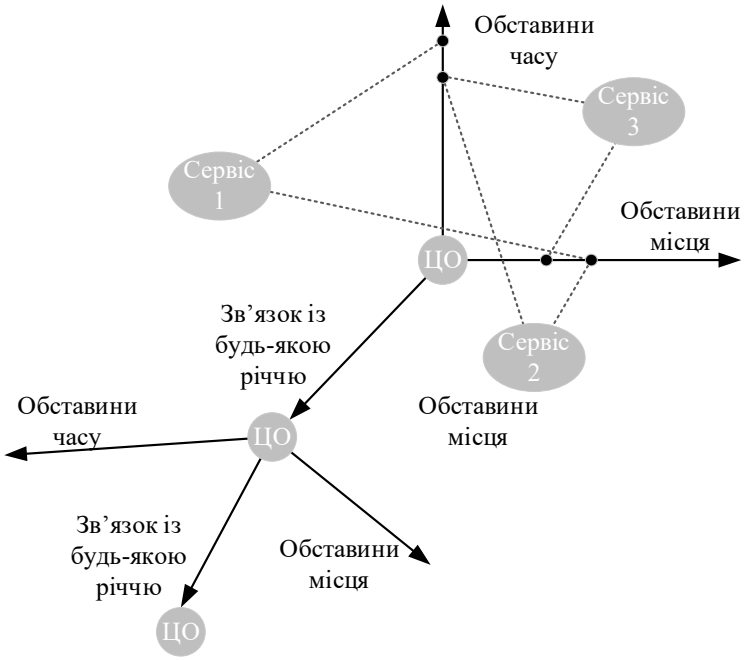

Рис. 2. Аспекти обставин, що додаються при розгляді зв’язку ЦО із сервісами згідно з Рекомендаціями МСЕ

На рисунку 3 показано, що з тих самих обставин місця і ситуації, але за різних обставин часу ЦО (також визначаючи обставини та інших координатах) ЦО може сформувати критерій вибору отримання різних сервісів.

Питання зав’язків сутностей (фактор «зв’язок із будь-якою річчю»), якими є ЦО, вирішується на рівні графів їх взаємозв’язків і не має прямого впливу на вибір сервісу та послуг у рамках сервісу, проте може визначати політики обмежень, які не дозволять при певних взаємозв’язках здійснити вибір того чи іншого сервісу.

Для того, щоб керувати поточним процесом вибору сервісу, а також беручи до уваги як було зазначено вище, що сервіс є цифровим об’єктом, необхідно здійснювати управління властивостями ідентифікаторів ЦО, а також процесом ідентифікації.

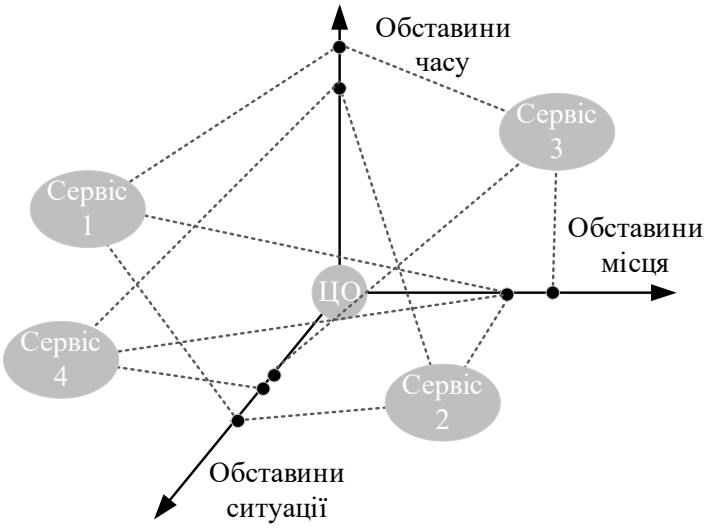

Рис. 3. Триплет обставин, відповідно до яких необхідно розглядати вибір умов надання послуг ЦО

Поділ цих двох процесів управління в рамках єдиного управління ідентифікації має принциповий характер, оскільки дозволяє ставити питання про поділ управління двома інформаційними потоками: потоком ідентифікації (ID flow) та потоком даних (data flow).

Поділ цих потоків дає можливість сформувати новий архітектурний підхід, який насамперед стосується вирішення питання, на якому рівні еталонної моделі (див. рис. 1) знаходиться функціонал управління ідентифікацією. Для його вирішення в еталонну модель необхідно ввести новий рівень – рівень управління ідентифікацією з виділенням на ньому двох функціоналів: управління властивостями ідентифікаторів та управління процесами ідентифікації (див. рисунок 4).

Слід визнати логічним розташування рівня управління ідентифікацією між рівнем управління мережного функціоналу та рівнем підтримки послуг і застосувань, тобто рівнем керування серверами. Це дає можливість визначити місце процесів ідентифікації яке пов’язує всі рівні в процесі обробки потоків даних.

Введення поняття триплету обставин {"часу", "місця", "ситуації"}, а з іншого боку, вміння управління властивостями "розумних" ідентифікаторів, створюють базу для формулювання умов для завдання персоналізації надання послуг.

Застосування триплету обставин {«часу», «місця», «ситуації»}, поділ управління властивостями ідентифікаторів та процесами ідентифікації дозволяє висунути гіпотезу, про існування правила умов при дотриманні яких завдання надання та надання сервісів у мультисервісній екосистемі завжди буде вирішуваною:

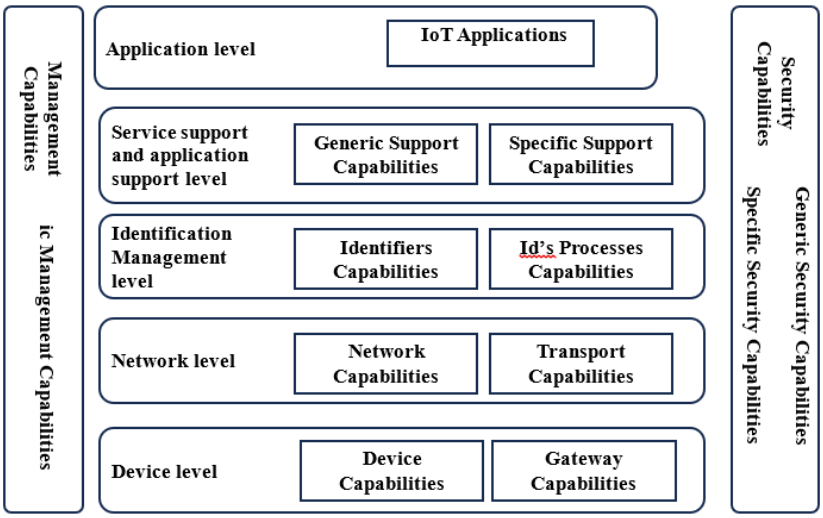

Рис. 3. Модифікована еталонна модель IoT

Формування архітектури надання послуг у мультисервісному середовищі, за яких цифровий об’єкт може:

1) їх персоналізувати,
2) визначити необхідність виклику,
3) сформувати умови надання,
4) розраховувати на їх надання залежно від обставин, у яких він перебуває

визначається дотриманням умов, коли:

1. будь-який користувач
2. в будь-який час
3. у будь-якому місці
4. в будь-якій ситуації
5. використовуючи будь-який власний ідентифікатор(и)
6. використовуючи власний пристрій(ї)
7. може отримати від будь-якого обраного оператора
8. необхідну йому персоналізовану послугу за умовами «тут і зараз»

Висновки

Матеріал, викладений у статті, дозволяє створити базу для розгляду принципів нової архітектури проектування інформаційних систем або комп'ютерних систем, що дозволяють гнучке управління цифровими об'єктами, їх властивостями, ідентифікацією цифрових об'єктів, властивостями ідентифікаторів залежно від обставин часу, місця та ситуації, у яких знаходяться цифрові об'єкти.

Також властивістю нової архітектури стає можливість інтеграції нових сутностей у інформаційні системи без значних модернізацій, пов'язаних із зміною вихідного та об'єктного коду, інформаційних схем систем, зокрема комп'ютерних систем модернізації структур даних, що призводять до необхідності обов'язкової реструктуризації таблиць баз даних та процедур управління таблицями баз даних.

Список використаної літератури:

1. Recommendation ITU-T Y.4403 (07/2012). Functional requirements and architecture of the next generation network for support of ubiquitous sensor network applications and services.

2. Recommendation ITU-T Y.4000 (06/2012). Overview of the Internet of things.

3. Recommendation ITU-T X.1252 (04/2021). Baseline identity management terms and definitions.

4. ETSI TR 103 719 V1.1.1 (2022-03). Guide to Identity-Based Cryptography.

5. ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT

6. RFC 7642. System for Cross-domain Identity Management: Definitions, Overview, Concepts, and Requirements. September, 2015

7. RFC 7643. System for Cross-domain Identity Management: Core Schema, September, 2015

8. RFC 7644. System for Cross-domain Identity Management: Protocol, September, 2015

9. 3GPP TS 24.382 V13.1.0 (2016-06) Technical Specification. 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mission Critical Push To Talk (MCPTT) identity management; Protocol specification (Release 13).

10. 3GPP Specification #: 33.924. Identity management and 3GPP security interworking; Identity management and Generic Authentication Architecture (GAA) interworking. Technical Report. (Release 9)

Автори статті

Вишнівський Віктор – доктор технічних наук, професор, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Каргаполов Юрій – старший викладач, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Єрмоленко Вадим – старший викладач, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Чичкарьов Євген - доктор технічних наук, професор, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

Authors of the article

Vyshnivskyi Viktor - Doctor of Science (technic), Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.

Karhapolov Yuriy - Senior Lecturer, State University of Information and Communication Technologies, Kyiv, Ukraine.

Yermolenko Vadim - Senior Lecturer, State University of Information and Communication Technologies, Kyiv, Ukraine.

Chychkarov Eugene - Doctor of Science (technic), Professor, State University of Information and Communication Technologies, Kyiv, Ukraine.