https://doi.org/10.31891/2219-9365-2022-72-4-1
УДК 621.391

Микола ВАСИЛЬКІВСЬКИЙ
Вінницький національний технічний університет
https://orcid.org/0000-0002-6586-2563
e-mail: mvasylkivskyi@gmail.com
Діана НІКІТОВИЧ
Вінницький національний технічний університет
e-mail: diananikitovych@gmail.com
Ольга БОЛДИРЕВА
Вінницький національний технічний університет
e-mail: rtt13bpoludenko@gmail.com

# КЕРУВАННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНИХ ДАНИХ В ІНТЕЛЕКТУАЛЬНИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

*Досліджено технології побудови інтелектуальних інфокомунікаційних мереж 6G у форматі цифрових платформ наступного покоління, які запропонують цифрові послуги з повним охопленням. Визначено ключову особливість систематичної структури керування даними, яка реалізує загальні підходи до даних, забезпечуючи прозору, ефективну, внутрішню безпеку та захист конфіденційності для внутрішніх та зовнішніх операцій в мережі 6G. Розглянуто основні концепції та відповідні мережеві функції та послуги.*

*Розглянуто інтелектуальну систему керування інформаційним захистом даних. Зокрема, досліджено сценарії керування даними в мережах 6G при участі кількох користувачів, які можуть бути потенційними споживачами даних, тобто споживати інформаційні дані або знання, надані системою 6G, або можуть бути постачальниками даних системи 6G. При цьому, мережа 6G може мати власну структуру керування доступом до даних, але, з іншого боку, технологія 6G також може реалізувати структуру керування даними разом з іншими учасниками галузі на основі їх власних знань у предметній галузі.*

*Досліджено схему інтегрованої архітектури керування захистом даних на основі технології розподіленого реєстру (DLT) для інтелектуальної радіомережі 6G. При цьому, технологія DLT знаходиться в ядрі системи мобільного зв'язку наступного покоління за допомогою відкритої екосистеми та формує новий рівень керування, що забезпечує самодостатню схему ідентифікації, отже автентифікація може виконуватися безперешкодно у різних доменах. Рівень керування даними та доступу до даних (DM/DA) створений для керування мережними та даними користувача і підтримує обмін сегментованими даними при збереженні вбудованої конфіденційності в декількох доменах.*

*Досліджено властивості технології DLT для досягнення трьох основних принципів проектування відкритої багатосторонньої екосистеми, а саме відкритості, функціональної сумісності та благонадійності. Оскільки будь-яка спроба доступу до даних та інформації через сервіси DLT буде реєструватися в реєстрі, властивість перевірки має ключове значення для реалізації принципу відкритості. При цьому, функціональна сумісність гарантує перетворення мережі 6G на багатосторонню екосистему, що забезпечує спільне надання послуг. Використання смарт-контракту дозволяє зовнішнім учасникам отримувати доступ через API до спільно використовуваних даних з іншого домену відповідно до умов, визначених власником даних. Крім того, запущений смарт-контракт (API) виконуватиметься автоматично, що сприяє функціональній сумісності в інтелектуальних інфокомунікаційних мережах.*

*Ключові слова: інтелектуальна інфокомунікаційна мережа 6G, цифрова платформа наступного покоління, інформаційний захист даних, інтегрована архітектура керування захистом даних, відкрита багатосторонняї екосистема, смарт-контракт, функціональна сумісність.*

Mikola VASYLKIVSKYI, Diana NIKITOVYCH, Olha BOLDYREVA
Vinnytsia National Technical University

# MANAGEMENT OF ACCESS TO INFORMATION DATA IN INTELLIGENT INFO-COMMUNICATION NETWORKS

*Technologies for building intelligent 6G information and communication networks in the format of next-generation digital platforms that will offer digital services with full coverage have been studied. A key feature of a systematic data management framework that implements common data approaches is identified, providing transparent, efficient, internal security and privacy protection for internal and external 6G network operations. Basic concepts and related network functions and services are covered.*

*The intelligent system of managing informational data protection is considered. In particular, the scenarios of data management in 6G networks with the participation of several users who can be potential data consumers, that is, consume information data or knowledge provided by the 6G system, or can be data providers of the 6G system, are investigated. At the same time, the 6G network may have its own data access management structure, but on the other hand, the 6G technology can also implement the data management structure together with other industry participants based on their own knowledge in the subject area.*

*The scheme of an integrated data protection management architecture based on distributed ledger technology (DLT) for the 6G intelligent radio network is studied. At the same time, DLT technology is at the core of the next-generation mobile communication system through an open ecosystem and forms a new management layer that provides a self-sufficient identification scheme, so authentication can be performed seamlessly in different domains. The Data Management and Data Access (DM/DA) layer is designed to manage network and user data and supports the exchange of segmented data while maintaining built-in privacy across multiple domains.*

*The properties of DLT technology to achieve the three main design principles of an open multilateral ecosystem, namely*

*openness, interoperability, and trustworthiness, are explored. Since any attempt to access data and information through DLT services will be registered in the registry, the verification property is key to realizing the principle of openness. At the same time, interoperability guarantees the transformation of the 6G network into a multilateral ecosystem that provides joint provision of services. The use of a smart contract allows external participants to access shared data from another domain through an API under conditions defined by the data owner. In addition, the launched smart contract (API) will be executed automatically, which promotes interoperability in intelligent information and communication networks.*

*Keywords: 6G intelligent information communication network, next-generation digital platform, information data protection, integrated data protection management architecture, open multilateral ecosystem, smart contract, interoperability.*

## Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

До появи технології 5G у попередніх поколіннях мобільного зв'язку використовувалась відносно закрита екосистема, в якій різні бізнес-суб'єкти взаємодіяли один з одним тільки в разі потреби. Наприклад, роумінг потребує співпраці кількох операторів мобільного зв'язку для усунення технічних обмежень. Така співпраця зазвичай передбачала кропіткі закриті переговори щодо контрактів, які охоплювали широкий спектр технічних, ділових та юридичних аспектів. Метою впровадження технології 5G було розширення екосистеми у бік вертикальних галузей. Тому було вирішено побудувати систему, яка залучає різні типи клієнтів шляхом розкриття можливостей мережі та відповідних інтерфейсів, наприклад, зосередивши увагу виключно на мережевих функціях.

Очікується, що мережа 6G стане цифровою платформою наступного покоління, яка запропонує цифрові послуги з повним охопленням. Для уніфікації широкого спектру послуг, необхідно залучити користувачів з різних областей, включаючи галузь інформаційних та комунікаційних технологій (ІСТ), а також всі інші вертикальні галузі. Цей процес об'єднання вже відбувається, хоч і перебуває в початковому стані та буде продовжувати розвиватись у майбутньому.

Нові користувачі поряд із звичайними операторами мобільного зв'язку сформують різноманітну екосистему 6G, яка має бути відкритою: фундаментальна вимога до архітектури – для забезпечення технічного та ділового співробітництва у розрахованому на багато користувачів середовищі. Крім того, така співпраця має бути ефективною, прозорою і заслуговувати на довіру. Відкрита екосистема також може стимулювати появу нових бізнес-моделей, що розраховані на багатокористувацьке співробітництво.

Телекомунікаційна система 6G є відкритою для широкого кола користувачів для однакової їх участі у розвитку, керуванні та експлуатації мережі та отримання прибутку від власних бізнесів. Це означає, що існуюча базова парадигма багатокористувацької взаємодії, що заснована на контрактах або взаємодії мережевих функцій не підходить для мережі 6G. Натомість мережа 6G модифікується до більш глибокої парадигми багатосторонньої участі та буде представлена як цифрова платформа інфокомунікаційних послуг наступного покоління для всього суспільства. Але для цього необхідно вирішити кілька ключових проблем, які заважають всій галузі ІСТ. Присутність розмежування між системами, оскільки мережева система за своєю суттю нині є закритою системою з приватною базою даних, політикою керування та логікою роботи служб. При керуванні ідентифікацією користувачів облікові дані користувачів є приватними даними, які постачальники послуг розміщують у сховищах даних, що перешкоджає можливості обміну інформацією. Висока собівартість співпраці та взаємодії, оскільки співпраця можлива лише після того, як обидві сторони обговорять взаємоприйнятні умови та підпишуть контракт, що є трудомістким та тривалим процесом. Однак навіть із підписаними контрактами, як і раніше, виникає безліч практичних питань через нечіткі критерії та непорозуміння. Відсутність довіри між користувачами мережі, але пряма взаємодія можлива, лише залишаються потенційні ризики, а це означає, що учасники угоди не хочуть або не можуть повністю довіряти один одному. У таких ситуаціях зазвичай залучають посередника – довірену третю сторону. Залежність від третьої сторони зумовлює додаткові операційні витрати, знижує ефективність, і навіть надає третій стороні надмірні повноваження. Мережа 6G по своїй суті буде багатокористувацьким мережевим середовищем і бізнес-екосистемою. При цьому, необхідно забезпечувати надійність та безпеку взаємодії між різними учасниками, а також гнучкість створення та припинення безпечних з'єднань між ними. Отже, подолання вищезгаданих проблем при проектуванні архітектури мережі 6G є фундаментальною вимогою для переходу до парадигми багатосторонньої участі та досягнення дійсно відкритої екосистеми.

## Аналіз досліджень та публікацій

Інформаційні дані мають ключове значення в сучасному цифровому суспільстві, тому в інфокомунікаційних системах 6G створюватимуться, збиратимуться та переміщатимуться величезні обсяги даних, які будуть застосовуватися для різних цілей експлуатації та керування, включаючи моніторинг показників, налаштування та протидії збоям, а також використовуватимуться для обміну знаннями з іншими системами та бізнес-секторами, сприяючи створенню ширшого діапазону споживчої цінності. Тільки за цих умов системи мобільного зв'язку стануть ключовим фактором подальшого розвитку інших галузей, зокрема промисловості [1].

Концепція керування даними включає збирання даних, їх обробку та зберігання, а також розвиток відповідної інфраструктури для отримання та використання високоякісних даних як ключових активів організації за допомогою відповідних процесів та технологій [2]. В даний час дані, що генеруються в системі мобільного зв'язку кожного оператора мобільної мережі, ізольовані та зберігаються окремо відповідно до технічних областей, наприклад RAN, базова мережа (CN), транспортна мережа (TN), OA&M та кінцеві пристрої [3]. Даним, що належать різним мережевим сегментам та користувачам, не вистачає відкритості та прозорості, що призводить до появи розрізнених сховищ, які є серйозною перешкодою для збору та обміну даними [4]. З іншого боку, великі компанії, що надають послуги поверх мереж мобільного зв'язку, накопичили великий досвід у галузі керування даними та стратегії монетизації (наприклад, у галузі зберігання даних, аналітичних послуг, багатих інтерфейсів прикладного програмування), які набагато розвиненіші, ніж сектор телекомунікацій. Схема керування даними у телекомунікаційній системі 6G має важливе значення для забезпечення надійної підтримки штучного інтелекту (ШІ) та сервісів сканування, тому очікується поява нових підходів та системних функцій [5].

**Формулювання цілей статті**

Метою роботи є: розроблення способів підвищення ефективності керування та обміну інформаційними даними в інфокомунікаційних мережах за рахунок використання технології розподіленого реєстру.

**Виклад основного матеріалу**

Керування даними виходить далеко за межі звичайного збору та зберігання даних. Загалом під час проектування системи керування даними необхідно враховувати чотири аспекти, що представлені на рис. 1.


**Рис. 1. Ключові аспекти системи керування даними в інфокомунікаційних мережах**

Доступність та якість інформаційних даних є одною із найсерйозніших проблем при застосуванні сервісів штучного інтелекту у різних галузях. Підвищення доступності даних передбачає збирання даних не тільки з одного сегмента однієї системи, але і з кількох сегментів різних систем. Отже, постає фундаментальне питання можливості подолання фізичних кордонів (наприклад, між різними типами обладнання, різними операторами та різнорідними галузями) для утворення єдиного інформаційного простору даних.

Після того, як розрізнені та ізольовані дані зібрані та доступні для використання, постає питання про те, як контролювати та покращувати якість даних. Доступність великих обсягів даних не означає, що інформаційні дані є якісними чи придатними для використання. Тому, необхідно реалізувати ефективну обробку даних за одночасного зниження складності обчислень та енергоспоживання.

При цифровізації суспільства важливість суверенітету, безпеки та конфіденційності даних стає безпрецедентною. Для регулювання процесу керування даними, багато країн ухвалили закони або постанови про захист конфіденційності. При цьому, постачальники інформаційних послуг також оновлюють свої схеми захисту конфіденційності. Крім того, уряди розвинених країн у всьому світі розробляють або публікують правила керування даними. При проектуванні системи 6G необхідно використовувати критерії оцінювання внутрішнього значення даних, щоб гарантувати забезпечення надання послуг належної якості, а також захистити конфіденційність з метою дотримання суверенітету даних, особливо у різних географічних регіонах.

Знання можна розглядати як оброблені дані, що мають певне призначення та цінність, а також їх можуть безпосередньо використовувати фізичні та віртуальні об'єкти, що діють у різних технічних та ділових галузях. Процес керування знаннями охоплює створення, оновлення та розкриття знань. При отриманні та оновленні знань необхідно ретельно аналізувати джерело та якість даних, а також вживати запобіжних заходів проти ненадійних або навіть зловмисних джерел неякісних або шкідливих даних. Розкриття інформаційних даних залежить від відповідної платформи та пристрою інтерфейсу.

Зібрані та задіяні інформаційні дані стають все більш складними та конфіденційними і часто включають пряму трансляцію інформації з датчиків та інших джерел. Збільшення кількості різноманітних джерел інформації призвело до появи нових потоків даних та нових типів контенту, що викликають політичне та юридичне занепокоєння щодо можливих зловживань, зокрема організації або уряди можуть використовувати ці можливості для контролю над суспільством. Так само нові технологічні можливості

заважають звичайним людям розрізняти справжній та шахрайський технологічний контент, такий як справжнє відео і дипфейк (deep fake; зображення або звук, виготовлені за допомогою глибоких нейромереж). Тому перед розробниками вже сьогодні стоїть завдання підтримувати чіткий баланс між збереженням соціальних вигод від передових технологій та ризиком небажаного перетворення цих нових технологічних можливостей на інструменти для контролю над суспільством та обмеження волі. Для виявлення витонченого шахрайства та запобіганню зловживанню передовими технологічними можливостями, необхідно розробити радикальніші правові та політичні інструменти.

Ключовою особливістю систематичної структури керування даними є незалежний рівень даних (рис. 2), який реалізує загальні підходи до даних, забезпечуючи прозору, ефективну, внутрішню безпеку та захист конфіденційності для внутрішніх та зовнішніх операцій в мережі 6G. Розглянемо основні концепції та відповідні мережеві функції та послуги.

Незалежний рівень даних призначений реалізації схеми керування даними у системі 6G. На рівень даних впливають усі можливі джерела інформації, повний цикл керування даними, включаючи створення/збір, зберігання, обробку та аналітику даних, а також надання готових до використання даних. Отже, незалежний рівень даних може надавати послуги передачі даних для зовнішніх бізнес-структур, таких як вертикальні галузі (наприклад, автомобілебудування, виробництво споживчих товарів та електронна охорона здоров'я), а також для самої системи 6G (наприклад, рівень керування, рівень користувача та рівень адміністрування), для автоматизації та оптимізації інфокомунікаційної мережі. Дані можуть включати конфігурації, стани та журнали, що пов'язані з мережевими операціями, особистими даними користувачів, даними датчиків і службовими даними, що надаються іншими учасниками.

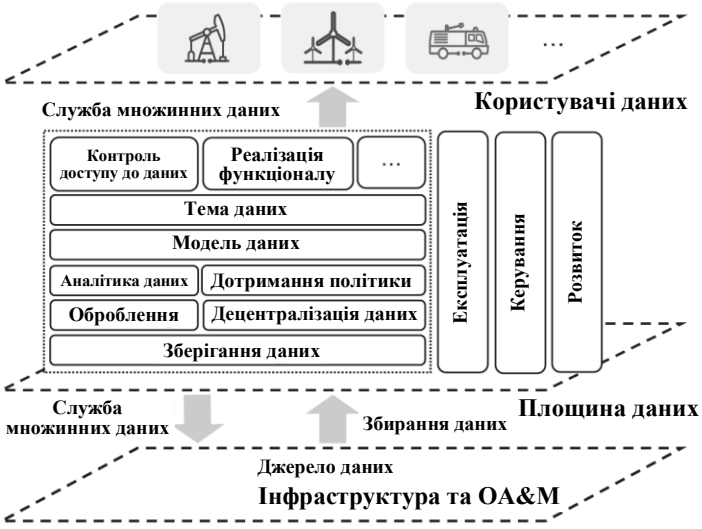


**Рис. 2. Незалежний рівень даних, необхідний для повної керованості**

Зібрані дані утворюють великий ресурс, який можна організувати за розподіленим принципом. При цьому, інформаційні дані зазвичай необхідно попередньо обробити (наприклад, виконати анонімізацію, приведення до заданого формату, шумозаглушення, перетворення та визначення ознак), перш ніж їх можна буде використовувати, оскільки пряме використання необроблених даних для таких додатків, як ШІ та сканування є досить проблематичним.

Для забезпечення цілісності та законності використання інформаційних даних під час їх обробки необхідно за умовчанням застосовувати встановлені законами та супутніми нормами політики щодо даних, що охоплюють географічні обмеження, національні чи регіональні правила конфіденційності та інші правила. Усі операції на рівні даних повинні відповідати правам та обов'язкам користувача даних, зазначеним у контракті на інформаційні дані. Крім того, рівень даних повинен забезпечувати десенсибілізацію даних, яка є ключовою умовою забезпечення захисту конфіденційності даних.

Усі послуги, що надаються згаданим рівнем даних, обслуговуються та керуються автономною системою OA&M.

Іншим важливим аспектом рівня даних є здобуття знань на основі збору, обробки та узгодження даних. Цей процес має виконуватися відповідно до вимог контракту для організування юридично бездоганної обробки та передачі відповідних інформаційних даних із кількох джерел.

Сама структура керування даними може постійно розвиватися і збагачуватися за рахунок нових джерел, моделей і даних, які підтримуються та використовуються клієнтами. Отже, вона допускає розробку інструментарію в реальному часі паралельно з експлуатацією наявних інструментів.

Оскільки рівень даних є логічною концепцією, він може бути реалізований із централізованою ієрархічною архітектурою. В якості альтернативи він може бути реалізований як логічна функція та розподілений граничними вузлами. Розглянемо деякі ключові компоненти даних.

Екосистема керування даними включає подвійні ролі: замовник даних / постачальник даних та власник даних / розпорядник даних, які можуть належати одним і тим самим або різним суб'єктам господарювання. Отже, у типовому сценарії керування даними в мережах 6G беруть участь кілька користувачів, які можуть бути потенційними споживачами даних, тобто споживати інформаційні дані або знання, надані системою 6G, або можуть бути постачальниками даних системи 6G. Мережа 6G може мати власну структуру керування даними, але, з іншого боку, технологія 6G також може реалізувати структуру керування даними разом з іншими учасниками галузі на основі їх власних знань у предметній галузі. Можливі різні шляхи еволюції (чи революції). Тому важливо ще на етапі розробки встановити, як права на дані розподілятимуться між різними бізнес-об'єктами на етапі експлуатації. Цього можна досягти за допомогою децентралізованих технологій, таких як блокчейн. Проте, будучи новим компонентом систем мобільного зв'язку, незалежні рівні даних можуть вимагати вироблення стандартизованих вимог до функцій та інтерфейсів.

Ресурс даних являє собою всю різноманітність даних, включаючи структуровані або неструктуровані дані, а також попередньо оброблені, післяоброблені чи необроблені дані.

Ефективний збір даних (наприклад, стану мережі та поведінки користувачів, таких як моделі їх мобільності) з бездротового середовища є первинною основою керування даними. Після чого можна використовувати ШІ для аналізу даних та надання отриманих знань внутрішнім або зовнішнім клієнтам. Тому важливо розуміти характер та властивості джерела даних.

На рис. 3 показані деякі з основних категорій джерел даних у системі 6G.

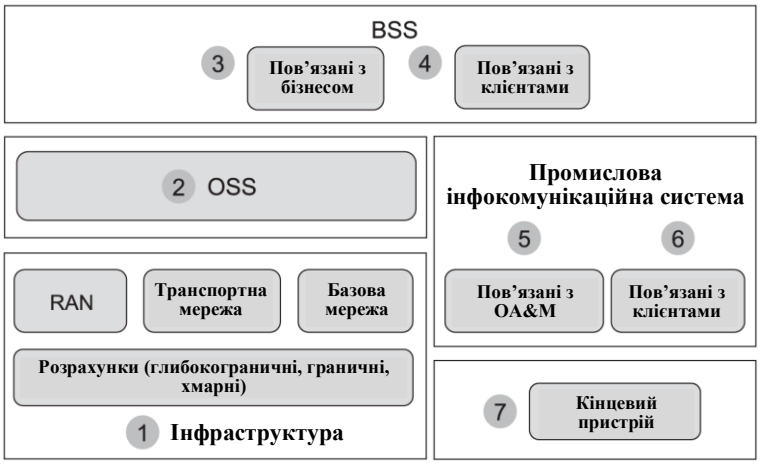


**Рис. 3. Основні категорії джерел даних**

Телекомунікаційна інфраструктура охоплює систему зв'язку та включає всі типи фізичних та віртуальних ресурсів, такі як RAN, TN та CN. Сюди також входять обчислювальні ресурси, включаючи хмарні, граничні та глибокі граничні обчислення. Дані, що стосуються інфраструктури, в основному генеруються всередині телекомунікаційної інфраструктури, включаючи обчислювальні ресурси, ресурси зв'язку (наприклад, стан мережевої послуги), інформацію сканування (наприклад, з RAN) та певні профілі користувачів (наприклад, інформацію про мобільність, місцезнаходження та зв'язаний контекст).

Система підтримки експлуатації (OSS) містить усі дані, пов'язані з експлуатацією та обслуговуванням (OA&M), такі як стан фізичного обладнання, інформацію про роботу системи та інформацію про надання послуг. Система підтримки бізнесу (BSS) містить усі дані, пов'язані з бізнес-логікою, наприклад, інформацію про керування відносинами з клієнтами та партнерами, а також дані про передплати як споживачам, так корпоративним клієнтам. При цьому, клієнти повинні повністю володіти такими даними та відповідно мати повний контроль над ними.

Галузева система зв'язку підтримує впровадження технології 6G в промисловий сектор, в якому зібрані дані можуть містити інформацію, що стосується промислового варіанту використання OA&M, а також можуть містити такі дані, як профілі промислових користувачів (наприклад, параметри трафіку та мобільності) та бізнес-дані / дані про послуги, що зберігаються у хмарі. Промислові замовники мають повністю володіти даними цього типу. Дані кінцевого обладнання включають обчислювальні та комунікаційні ресурси пристрою, профілі використання послуг та інформацію про сканування. При цьому, кінцеві користувачі повинні повністю володіти цими даними.

У мережах 6G одною з основних ролей керування даними є надання відповідних методів для створення ресурсів даних, що потребує наявності відповідної архітектури, а також підтримки мережевих функцій. Першим кроком в цьому напрямку є збір даних. Ключові кроки збору даних полягають у наступному: встановлення угоди (наприклад, авторизація на право збору даних) та встановлення безпечного з'єднання з джерелом даних; отримання вимог щодо збору даних; ухвалення рішення, які дані збирати, а також де, коли і як збирати дані відповідно до вимог; повідомлення джерела даних про атрибути даних; збір даних із джерела та збереження їх у базі даних; керування та підтримка працездатності бази даних.

Керування ресурсом даних відкриває можливість надання аналітики даних як послуги для різних типів клієнтів. При цьому, можуть застосовуватися чотири типи аналітики: описова аналітика збирає статистичну інформацію про історичні дані, щоб забезпечити розуміння мережі, наприклад, швидкодію мережі, профіль трафіку, стан каналу та кількість користувачів; діагностична аналітика дозволяє автономно виявляти мережеві збої та порушення обслуговування, виявляє основні причини мережевих аномалій та зрештою підвищує надійність та безпеку мережі; прогностична аналітика використовує дані для прогнозування майбутніх подій, таких як моделі трафіку, розташування користувачів, поведінку та переваги користувачів, доступність ресурсів і навіть збої; попередня аналітика використовує прогностичну аналітику для надання пропозицій щодо розподілу ресурсів, розміщення контенту тощо.

Послуги з аналізу даних генеруватимуть знання, отримані з рівня даних. Результат може містити проактивні знання (наприклад, рекомендації щодо дій) та пасивні знання (наприклад, обмін інформацією та дії, вжиті клієнтами).

Такий аналіз даних може бути зумовлений клієнтами та адаптований до їхніх вимог. При цьому, рівень даних повинен забезпечувати багатовимірне надання послуг та даних на запит. Збір та зберігання конфіденційних даних пов'язані з ризиком порушення конфіденційності та обов'язком захищати конфіденційність. Десенсибілізація даних необхідна для вирішення проблем конфіденційності, а також для дотримання правових норм, особливо для підтримки ШІ та завдань розпізнавання в рамках технології 6G.

Зокрема для завдань ШІ потрібно розглядати структуру з багатопрофільним доступом до даних (диференційований доступ). Останнім часом було проведено значну кількість досліджень диференційованої конфіденційності в області ШІ [5, 6], зосереджених на тому, як анонімізувати навчальні дані окремих пристроїв.

Десенсибілізація даних під час навчання моделі та виведення ШІ є важливим критерієм при проектуванні мережі 6G. Підходи, які можуть бути використані для забезпечення диференційованої конфіденційності, включають введення шуму в навчальні дані без шкоди для їх статистичних властивостей, щоб навчена модель, як і раніше, фіксувала ознаки у вихідному наборі даних [7], та застосування криптографічних методів, щоб навчання ґрунтувалося на зашифрованих (а не розшифрованих) даних [8]. Альтернативний підхід полягає в тому, що пристрої надсилають до мережі параметри моделі, а не навчальні дані. Два приклади цього підходу – федеративне навчання [9] та роздільне навчання [10].

Одна з ключових проблем полягає в тому, що зловмисний інсайдер з повним знанням режиму навчання може створити інформацію, аналогічну до навчальних даних, використовуючи поступову конвергенцію моделі [11]. Наприклад, при федеративному навчанні це може призвести до витоку інформації на зловмисні пристрої. Тому, важливо знати, як необхідно поводитися з різними типами методів навчання, а також враховувати їх обмеження, не знижуючи при цьому універсальність десенсибілізації даних. Для вирішення нових проблем необхідно застосовувати нові принципи проектування. Тому при проектуванні системи 6G необхідно враховувати три наступні принципи.

Принцип відкритості мережі 6G, яка повинна бути більш відкритою з точки зору обміну мережевою інформацією та знаннями, мережевих операцій та розкриття доступу до можливостей багатокористувацької спільної роботи. Ізоляція даних передбачає розподілення даних поточної системи на ізольовані домени, де дані зберігаються в приватному порядку і не використовуються спільно. І навпаки, відкритість принципово змінює спосіб обробки даних (як приватних, і загальнодоступних) користувачами мобільної мережі. Декілька користувачів з різних технічних та бізнес-областей повинні мати доступ до зберігання та обробки даних, що полегшує потік інформації через різні границі системи.

Підвищення відкритості інфокомунікаційної мережі гарантує, що переміщення та обробка інформації в одному або кількох доменах будуть більш прозорими. Сучасна мережева система сприймається як чорна скринька, де зовнішні користувачі мають доступ тільки до вихідних результатів. Така закрита система викликає закономірні побоювання щодо потенційних проблем із конфіденційністю та безпекою. Це не лише підриває довіру користувачів до мережевої системи, а й ставить під загрозу готовність різних користувачів ринку мережевих послуг брати участь у ній через відсутність інформації, необхідної для взаємодії на рівних.

Відкритість лише зберігає границю між сферами діяльності користувачів, а не усуває її разом із відповідними політиками контролю, але при цьому спосіб передачі буде радикально змінено. Крім того, відкритість приносить взаємний зиск за рахунок загальнодоступної інформації, не роблячи систему повністю прозорою.

В мережах 6G потрібно підвищувати рівень взаємодії для забезпечення очікуваних показників більшості сценаріїв використання, оскільки багато з них, передбачають суворі вимоги до якості послуги, такі як наднизька затримка. Така сумісність вимагає узгодженої роботи різних користувачів для динамічної оптимізації кількох доменів, а це означає, що міждоменні операції стануть нормою.

Функціональна сумісність у мережах 6G забезпечить безшовне міждоменне використання функцій під прямим контролем різних користувачів, на відміну від сьогоднішньої реалізації, яка надає лише інтерфейси обміну параметрами.

Принцип благонадійності зумовлює перетворення мережі 6G на децентралізовану екосистему, що відкрита для вільного входу та виходу різних користувачів. З точки зору багатосторонньої участі благонадійна система 6G повинна: забезпечити розраховану на багато користувачів структуру міждоменного керування інформаційними даними, в якій може бути реалізований детальний контроль доступу до даних; бути «точкою довіри» при наданні інформації декільком користувачам; забезпечити можливість аудиту наданих послуг, операцій та керування, наприклад через системні журнали, які мають бути автентичними та незаперечними. Ці три принципи проектування взаємопов'язані один з одним.

Розглянемо одну з ключових технологій, задіяних у створенні спільної багатосторонньої екосистеми, це технологію розподіленого реєстру (DLT). Очікується, що DLT стане основою запропонованих принципів проектування. Оскільки спільна екосистема буде розширюватися і охоплювати концепції, пов'язані як з бізнесом, так і з технологіями, вона включає всі відповідні мережеві функції, а саме мережевий ШІ, орієнтовану на користувача мережу, вбудовану благонадійність та інтегровані неназемні мережі. DLT надає ключові функції, необхідні для побудови нової системи мобільного зв'язку на основі відкритої, функціонально сумісної та надійної платформи. Така платформа залучить учасників з різних секторів, від уряду та освіти до охорони здоров'я та постачальників послуг, таких як фінанси та транспорт. Розглянемо ключові функції та об'єкти, на які впливає DLT.

За останнє десятиліття технологія блокчейна стала неймовірно популярною завдяки криптовалюті та глибокому впливу, який вона створила на сучасне цифрове суспільство. Основні концепції блокчейн-технології стали відомі після публікації протоколу Paxos [1], який заклав основу для створення біткоїну. Біткоїн, випущений розробником (або групою розробників) під псевдонімом Сатоші Накамото в 2008 році, є одноранговою системою електронних грошей, яка покликана виконувати роль публічного реєстру для транзакцій з криптовалютою. Наступного року було створено блокчейн криптовалюти біткоїн. Завдяки використанню блокчейну біткоїн повністю децентралізований, так що жоден користувач не може контролювати електронні гроші, і не існує єдиної точки відмови, що сприяє поширенню біткоїну. Основною перевагою біткоїну є можливість прямих трансакцій між користувачами без використання довіреної третьої сторони.

Крім використання в цифрових валютах, таких як біткоїн, з 2014 року технологія блокчейн застосовується в інших додатках, що працюють з використанням смарт-контрактів. Блокчейн 1.0, раніше застосовуваний тільки для додатків криптовалюти, згодом перетворився на блокчейн 2.0 і 3.0. Розвиток блокчейн-технології відкрив нові ринки та можливості: наприклад, децентралізовані додатки (Dapps) були неможливі з блокчейної версії 1.0. Блокчейн у поєднанні зі смарт-контрактами дозволяє вбудовувати бізнес-логіку та механізми бізнес-процесів у ланцюжок і крім біткоїнів обмінюватися й іншими цифровими активами. Основні переваги технології блокчейну вперше були реалізовані в індустрії цифрової економіки. Але з розвитком технології у блокчейну з'явився ряд переваг з погляду прозорої обробки транзакцій між різними бізнес-об'єктами. Ці переваги можуть бути використані при проектуванні архітектури мережі 6G, наприклад, для створення відкритої та спільної екосистеми, а також з метою забезпечення інформаційної безпеки.

Блокчейн можна використовувати як цифрову систему для запису транзакцій з активами у кількох місцях одночасно [12, 13]. На відміну від традиційних баз даних, розподілені реєстри немають централізованого сховища даних чи функцій адміністрування. Хоча терміни блокчейн і DLT часто використовуються як взаємозамінні, вони суттєво різняться у тому сенсі, що блокчейн є лише підмножиною технології розподіленого реєстру. Ключові властивості DLT полягають у наступному. Технологія DLT фактично використовує децентралізовану архітектуру, де кілька користувачів разом утворюють розподілену систему. Розподіленим консенсусом є ядро системи з урахуванням DLT. У процедурі розподіленого консенсусу записи розподіленого реєстру можуть переходити з одного стану до іншого без централізованого контролю. Кожна зміна стану підлягає демократичній процедурі голосування: після того, як більшість вузлів досягають угоди, новий стан приймається та глобально синхронізується на кожному вузлі. Це гарантує, що всі вузли системи на основі DLT завжди мають глобальну інформацію про систему.

Процедура розподіленого консенсусу забезпечує незмінність записів у системі на основі DLT [14]. Протокол розподіленого консенсусу (наприклад, Proof-of-Work у біткоїні) влаштований таким чином, що неможливо з обчислювальної точки зору підробити записи реєстру, якщо тільки не скомпрометовано більшість вузлів. Залежно від того, який розподілений протокол використовується, частка скомпрометованих вузлів, що необхідні для забезпечення обчислювальної можливості підробки,

коливається від 30% до 51% [5, 6]. Процедура розподіленого консенсусу забезпечує можливість аудиту. Реєстр містить усі записи історичного стану, тому що додавання нового запису до наявного є єдиним способом оновлення реєстру. Завдяки властивості незмінності кожен вузол має повну копію записів, що дозволяє проводити локальний аудит.

Смарт-контрактом є виконавчий двійковий код, який застосовує задану в коді логіку обробки до записів реєстру. Одна з основних відмінностей між смарт-контрактом та звичайним додатком полягає в тому, що виконання смарт-контракту надійно гарантоване та повністю автоматизоване. Тому, при дотриманні наперед визначених умов виконання смарт-контракту не може бути перервано.

Крім визначення логіки обробки записів, що зберігаються у реєстрі, смарт-контракт також надає набір API. Користувачі можуть викликати ці API, щоб запустити смарт-контракт, надіславши транзакцію до смарт-контракту. Після публікації смарт-контракту в системі на основі DLT він фіксується у розподіленому реєстрі кожного вузла системи, після чого стає загальнодоступним та незмінним.

Ключові властивості технології DLT можуть бути використані для досягнення трьох основних принципів проектування відкритої багатосторонньої екосистеми, а саме відкритості, функціональної сумісності та благонадійності. Відкритість забезпечує простий спосіб обміну даними та інформацією між кількома доменами 6G. Використання розподіленого консенсусу дозволяє обмінюватися даними та інформацією по всьому світу без централізованої третьої сторони. У той самий час властивість незмінності допомагає забезпечити цілісність загальних даних та інформації. Оскільки будь-яка спроба доступу до даних та інформації через сервіси DLT буде реєструватися в реєстрі, властивість перевірки має ключове значення для реалізації принципу відкритості. При цьому, функціональна сумісність гарантує перетворення мережі 6G на багатосторонню екосистему, що забезпечує спільне надання послуг. Використання смарт-контракту дозволяє зовнішнім учасникам отримувати доступ через API до спільно використовуваних даних з іншого домену відповідно до умов, визначених власником даних. Крім того, запущений смарт-контракт (API) виконуватиметься автоматично, що сприяє функціональній сумісності. Благонадійність спрямована на те, щоб зробити мережу 6G загальним гарантом довіри для зберігання даних, обміну інформацією та відповідальності за якість послуг. Властивість незмінності допомагає підвищити безпеку та надійність даних та інформації, що спільно використовуються в декількох доменах, у той час як розподілений консенсус підвищує надійність, оскільки різні користувачі повинні досягти згоди з питань зміни даних та розповсюдження інформації. Оскільки, зміна стану системи визначається у вигляді процедури демократичного голосування, яка надійно дотримується сумлінними користувачами.

Очікується, що в екосистемі 6G мобільна мережа діятиме як цифрова платформа, де кілька користувачів із різних доменів взаємодіють один з одним для надання послуг тій чи іншій стороні. Це потребує реалізації нових принципів проектування. При цьому, технологія DLT має низку перспективних властивостей, які напевно виявляться корисними при реалізації нових принципів проектування. Інтеграція технології DLT в мережу 6G забезпечить надання прозорих та децентралізованих мережевих функцій відповідно до нових принципів проектування. Однак, незважаючи на численні переваги, технологія DLT також має обмеження. Наприклад, у випадках, коли потрібно спільно використовувати великі обсяги даних, технологія DLT може спровокувати небажані явища, такі як зниження загальної пропускної спроможності телекомунікаційної системи, високу затримку та високе енергоспоживання. Тому, присутня необхідність продовження вдосконалення технології DLT. Покажемо особливості перетворення системи мобільного зв'язку наступного покоління за допомогою технології DLT.

Технологію DLT можна використовувати для створення нової схеми керування ідентифікацією та парадигми керування цифровими активами, в якій користувачі керують своїми власними цифровими активами, а коло користувачів варіюється від приватних споживачів до підприємств. Це допоможе спростити керування мережею та OA&M. Крім того, системи забезпечення експлуатації (OSS) і системи забезпечення бізнесу (BSS) на основі технології DLT стануть простіше, оскільки відпаде необхідність у сторонньому координаторі. Для платформи багатостороннього використання все перелічене є нагальною необхідністю.

На рис. 4 представлено базову схему DLT-інтегрованої архітектури для мережі 6G. Технологія DLT знаходиться в ядрі системи мобільного зв'язку наступного покоління за допомогою відкритої екосистеми. Фактично DLT – це основа, де буде побудовано новий рівень керування, що забезпечує самодостатню схему ідентифікації, отже автентифікація може виконуватися безперешкодно у різних доменах. Рівень керування даними та доступу до даних (DM/DA) створений для керування мережними та даними користувача і підтримує обмін сегментованими даними при збереженні вбудованої конфіденційності в декількох доменах. На основі цих двох рівнів можуть бути побудовані такі рівні керування мережею та OSS/BSS.

Інші учасники різних доменів також можуть приєднатися до коаліції мобільних мереж, створивши загальні рівні даних на основі технології DLT. Кожен користувач визначає власні політики спільного використання даних і надає смарт-контракт для реалізації логіки автономної обробки загальних даних у розподіленому реєстрі або в різних реєстрах.

Користувачі бажають контролювати свої дані та спілкуватися анонімно чи псевдонімно, щоб захистити свою особистість та конфіденційність. Для цього в доповнення до криптографічних механізмів інформаційного захисту даних потрібно застосовувати передові технології, такі як біометрія та DLT.

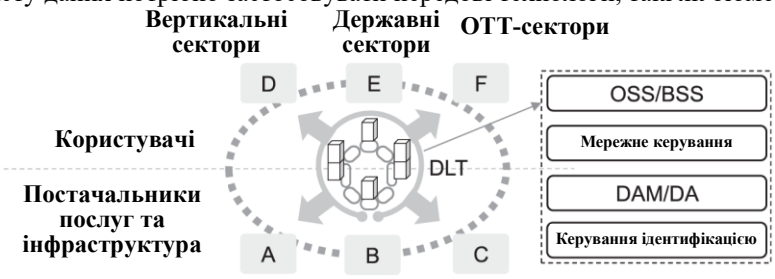


**Рис. 4. Узагальнена схема DLT-інтегрованої архітектури для мережі 6G**

У звичайній системі мобільного зв'язку користувачеві потрібна SIM-картка для використання мережі оператора. При купівлі модуля ідентифікації абонента (SIM-картки) користувач надає особисті дані, такі як дата народження, стать, адреса та спосіб виставлення рахунків. Це еквівалентно створенню облікового запису (тобто збереження облікових даних користувача) у базі даних оператора. Щоразу, коли користувач звертається до мережі, інформація користувача звіряється з інформацією, що зберігається у базі даних. Користувачу надається доступ до мережі лише у разі успішної перевірки. Кожен оператор зберігає такі облікові дані в центральному репозиторії даних користувача (UDR), який ізольований і належить тільки одному домену; однак очікується, що в телекомунікаційних мережах 6G цей механізм працюватиме інакше.

На рис. 5 показано передумови використання технології DLT шляхом реалізації схеми самодостатньої ідентифікації [7]. Зокрема, оператор після затвердження профілю користувача видає йому сертифікат. Сертифікат абонентського обладнання містить відкритий ключ користувача та підпис оператора. Після чого, оператор (наприклад, з домену А) публікує свій власний сертифікат домену, який містить відкритий ключ оператора до реєстру. Цей сертифікат є загальнодоступним для всіх. Для доступу іншого оператора (наприклад, з мережевого домену Б) до виконання аутентифікації, йому потрібно лише отримати сертифікат домену, виданий мережевим доменом А. В результаті, підпис сертифіката користувача може бути перевірений за допомогою отриманого відкритого ключа, і це буде підтверджувати, що сертифікат дійсно був виданий заявленим оператором -відправником та результативного здійснення аутентифікації користувача.

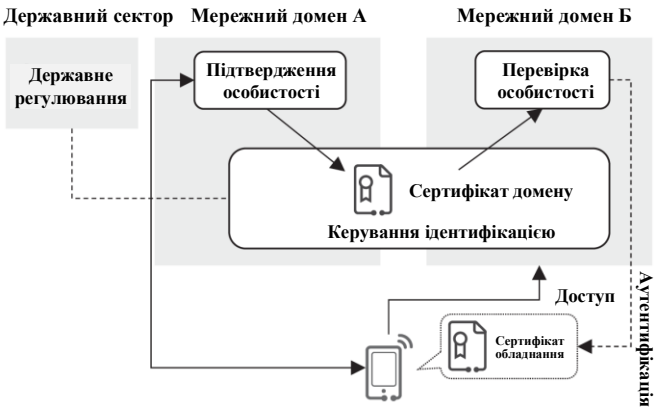


**Рис. 5. Керування ідентифікацією на основі технології DLT**

Механізм самостійної ідентифікації відкриває нові можливості для керування ідентифікаторами мобільної мережі. По-перше, закритий ключ може бути згенерований користувачем, а не створений у базі даних оператора. Оскільки для дешифрування може використовуватись лише закритий ключ, суверенітет особи належить власнику ідентифікатора (тобто користувачу). По-друге, оператор більше не функціонує як автор ідентифікатора, а як агент, що підтверджує особистість. Це звільняє оператора від необхідності зберігати великий обсяг конфіденційної інформації про користувачів, таких як імена користувачів та паролі. По-третє, будь-який оператор може перевірити ідентифікатор у сертифікаті, отримавши відповідний відкритий ключ, що означає, що автентифікація більше не обмежується окремими операторами.

Використовуючи схему керування ідентифікацією на основі технології DLT можна створити відкриту платформу для підтвердження особистості. У деяких випадках може бути зручніше чи вигідніше

підтверджувати особу на рівні державного чи міського органу влади, ніж звертатися до операторів, які виконують цю роль. Чим надійніший індосант (підтверджуюча сторона), тим авторитетнішою буде система ідентифікації.

Технологія DLT відіграє ключову роль у створенні єдиного надійного рівня даних для мобільної мережі 6G. За допомогою технології DLT користувачі можуть отримати більший контроль над своїми даними замість того, щоб дозволяти іншим користувачам (наприклад, постачальникам послуг на основі мережі мобільного зв'язку (OTT)) мати виняткову владу над ними. В результаті, всі користувачі матимуть ключі для доступу до своїх даних.

Керування даними на основі технології DLT та доступ до даних цифрових активів користувачів дозволяють їм керувати своїми власними активами, а також відкривають можливості для будівництва нової бізнес-моделі. Як показано на рис. 6 дані можуть бути легко і безпечно розділені між різними учасниками [8]. Зокрема, технологія DLT може допомогти двома способами: (1) встановити розподілений консенсус за опублікованими даними та (2) допомогти безпосередньо обмінюватися даними в автономному режимі, а також гарантувати цілісність вихідних даних.

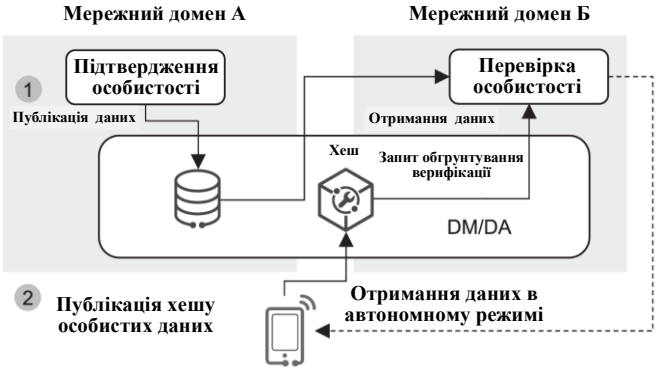


**Рис. 6. Схема керування доступом до інформаційних даних на основі технології DLT**

Для встановлення розподіленого консенсусу за опублікованими даними, дані безпосередньо публікуються та перевіряються всією мережею за допомогою протоколу розподіленого консенсусу. Кожна частина мережі використовує однакові облікові дані реєстру, що означає їх спільне використання в процесі розподіленого консенсусу. Однак, оскільки дані до реєстру можна лише додавати, пряма публікація даних у реєстрі викликає проблему стійкості рівня мережевих даних. Інша проблема полягає в тому, що оскільки опубліковані дані реплікуються на кожному вузлі та загальнодоступні, тому конфіденційність даних не може бути гарантованою. В результаті, цей підхід підходить лише для невеликої кількості даних, які є відносно статичними та нечутливими до розголошення.

Для забезпечення безпосереднього обміну інформаційними даними між користувачами в автономному режимі, а також гарантування достовірності вихідних інформаційних даних, у реєстрі публікують перевірочну інформацію (зазвичай хеш-значення) вихідних даних, а не самі дані. Для перевірки достовірності даних, одержувач може звернутися до опублікованої інформації. Крім того, дані переміщуються в автономному режимі між відправником і одержувачем (наприклад, мережевий домен Б приймає дані безпосередньо від обладнання користувача).

Керування інформаційними даними на основі технології DLT формує нову схему керування захистом та обміну даними у мобільній мережі 6G. По-перше, дані не обов'язково повинні зберігатися приватно в одному домені. Натомість дані можуть бути зашифровані та розповсюджені по всій мережі, оскільки технологія DLT гарантує їх достовірність. По-друге, конкретний механізм керування доступом може бути реалізований за допомогою смарт-контрактів. Будь-який запит на доступ до опублікованих даних шляхом запуску смарт-контракту буде записано, що полегшить інформаційний аудит. Це особливо важливо щодо даних, які використовуються для спільного керування, таких як стан мережі, контекст сеансу та вимоги QoS. Керування даними на основі технології DLT може перетворити рівень даних на децентралізований ринок даних, де відбувається прямий обмін цифровими активами між початковими власниками активів та користувачами. Використовуючи технологію DLT можна організувати повний децентралізований моніторинг доступу до даних, їх передачі та аудиту. Технологія DLT може знайти застосування у двох ключових аспектах керування телекомунікаційною мережею, а саме керування сеансом та керуванні доступом і мобільністю.

Під час керування сеансом маршрут переадресації для обладнання користувача на рівні користувача встановлюється відповідно до запиту сеансу обладнання. В даний час керування сеансом визначає маршрут переадресації на основі глобальної інформації про мережевий рівень або простих правил маршрутизації. Однак у системі 6G керування сеансом можуть здійснювати різні розподілені об'єкти керування у різних

доменах. Це ускладнює отримання глобальної інформації, і тому може знадобитися, щоб кілька об'єктів керування сеансом зв'язку обмінювалися мережевою інформацією один з одним, незалежно від того, чи вони знаходяться в одному домені. Технологія DLT сприяє вирішенню цієї проблеми шляхом ведення загального розподіленого реєстру, в якому різні керуючі об'єкти можуть публікувати мережеву інформацію зі свого власного домену. Для гарантування, що конфіденційну інформацію не буде розкрито, можна передбачити політики публікації. Сеанси можна створити в кількох доменах за допомогою смарт-контрактів, які публікуються різними об'єктами керування сеансом. Смарт-контракти визначають умови та вхідні дані, необхідні для створення маршруту переадресації у певному домені. Після виклику смарт-контракту технологія DLT гарантує його виконання, і відповідно розгортається сегмент маршруту. Щоразу, коли викликається смарт-контракт, всі операції записуються до розподіленого реєстру для перевірки. Ці переваги роблять технологію DLT ідеальним вибором для забезпечення спільного використання даних у кількох доменах мережі доступу.

Керування доступом та мобільністю (безперервність сеансу та послуг) стикається з проблемою, аналогічною тій, з якою стикається керування сеансом зв'язку, коли кількість об'єктів керування збільшується та об'єкти розподіляються в мобільній мережі 6G. У поточних реалізаціях керування доступом обладнання користувача аутентифікується шляхом запиту служби аутентифікації, яка взаємодіє з репозитарієм даних користувача (UDR), в якому запит загального ключа генерується службою аутентифікації користувача обладнання. При надходженні від обладнання запиту на доступ, служба керування доступом надає дозвіл доступу. При цьому, механізм запиту загального ключа використовує попередній ідентифікатор обладнання, який дешифрується службою автентифікації для отримання постійного ідентифікатора UE.

Технологію DLT можна використовувати, навіть якщо реалізовано традиційну схему аутентифікації із загальним ключем. При цьому, запит загального ключа може бути підготовлений заздалегідь відповідно до постійного ідентифікатора обладнання, що зберігається в UDR. Служба аутентифікації готує смарт-контракт, що перевіряє, і публікує його в розподіленому реєстрі, доступ до якого здійснюється набором відповідних об'єктів керування доступом. Будь-який об'єкт керування доступом може отримати підготовлений запит і відправити його в обладнання користувача. Потім обладнання, що запросило доступ, вирішує завдання та повертає своє рішення об'єкту керування доступом, який відправляє рішення до смарт-контракту. Аутентифікація обладнання проходить успішно якщо смарт-контракт підтверджує правильність рішення, що усуває необхідність у послідовній обробці запиту безліччю керуючих об'єктів, особливо коли мережева функція повинна бути обрана з безлічі NF-кандидатів. Цей підхід також працює у міждоменному сценарії, коли служби аутентифікації в різних доменах готують завдання та відповідні смарт-контракти перевірки. Процес аутентифікації відбувається так само, як і в сценарії з одним доменом, без будь-якого міждоменного обміну.

**Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі**

Досліджено альтернативний і найкращий підхід для керуванням доступу до інформаційних даних у форматі використання парадигми верифікації, що заснована на самостійному керуванні ідентифікатором. Визначено, що для абонентського телекомунікаційного обладнання із авторизованим оператором мережі сертифікат, оператор публікує його сертифікат у розподіленому реєстрі, який розповсюджується різними доменами. У цьому випадку обладнання підключається до об'єкта керування доступом і запитує доступ до мережі, одночасно надаючи сертифікат. Об'єкт керування доступом аналізує ідентифікатор домену (тобто дивиться, хто спочатку випустив сертифікат обладнання) та отримує сертифікат оператора з розподіленого реєстру. Потім об'єкт керування доступом перевіряє сертифікат обладнання. При цьому, відбувається успішна аутентифікація при результативній перевірці.

Досліджено особливості керування мобільністю телекомунікаційних пристроїв. Визначено, що під час передачі обслуговування (хендовера) власного обладнання об'єкт керування мобільністю використовує контекстну інформацію обладнання із врахуванням стану RAN спільно з об'єктом керування сеансом зв'язку. В результаті, запускається послідовна взаємодія та передача сигналів між кількома об'єктами керування мобільністю та сеансом зв'язку. Визначено технологію DLT як основу для побудови нового рівня керування, що забезпечує самодостатню схему ідентифікації, отже автентифікація може виконуватися безперешкодно у різних доменах. Досліджено можливість застосування технології DLT для реалізації стратегії попереджувального хендовера, згідно з якою створюється локальний кластер мережевих функцій для перемикання, і в результаті телекомунікаційне обладнання в цьому кластері може бути заздалегідь синхронізованим. При цьому скоротиться тривалість процесу передачі обслуговування, що необхідна для надсилання та створення нового контексту телекомунікаційного обладнання. Ефективна синхронізація в даному випадку цілком реалізована, оскільки такі кластери містять лише обмежену кількість локальних пристроїв користувача. Визначено, що багато мобільних мережних функцій мають аналогічні проблеми з адмініструванням сеансу та керуванням доступом та мобільністю. Тому, такі функції також можна перетворити для роботи на основі технології розподіленого реєстру даних.

**Література**

1. P. Vepakomma, T. Swedish, R. Raskar, O. Gupta, and A. Dubey, No peek: A survey of private distributed deep learning, arXiv preprint arXiv:1812.03288, 2018.

2. M. Minelli, Fully homomorphic encryption for machine learning, Ph. D. dissertation, 2018.

3. O. Gupta and R. Raskar, Distributed learning of deep neural network over multiple agents, Journal of Network and Computer Applications, vol. 116, pp. 1–8, 2018.

4. Z. Zheng, S. Xie, H. Dai, X. Chen, and H.Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in Proc. 2017 IEEE International Congress on Big Data. IEEE, 2017, pp. 557–564.

5. F. Hofmann, S.Wurster, E. Ron, and M. Böhmecke-Schwafert, The immutability concept of blockchains and benefits of early standardization, in Proc. 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K). IEEE, 2017, pp. 1–8.

6. Y. Zhu, Y. Qin, Z. Zhou, X. Song, G. Liu, and W. C.-C. Chu, Digital asset management with distributed permission over blockchain and attribute-based access control, in Proc. 2018 IEEE International Conference on Services Computing (SCC). IEEE, 2018, pp. 193–200.

7. Vladimir G. Krasilenko, Alexander A. Lazarev, and Diana V. Nikitovich "Modeling of biologically motivated self-learning equivalent-convolutional recurrent-multilayer neural structures (BLM_SL_EC_RMNS) for image fragments clustering and recognition", Proc. SPIE 10609, MIPPR 2017: Pattern Recognition and Computer Vision, 106091D (8 March 2018); https://doi.org/10.1117/12.2285797

8. Vladimir G. Krasilenko, Alexander A. Lazarev, and Diana V. Nikitovich "Design and simulation of optoelectronic neuron equivalentors as hardware accelerators of self-learning equivalent convolutional neural structures (SLECNS)", Proc. SPIE 10689, Neuro-inspired Photonic Computing, 106890C (21 May 2018); https://doi.org/10.1117/12.2316352

9. Vladimir G. Krasilenko, Alexander A. Lazarev, and Diana V. Nikitovich "Modeling and possible implementation of self-learning equivalence-convolutional neural structures for auto-encoding-decoding and clusterization of images", Proc. SPIE 10453, Third International Conference on Applications of Optics and Photonics, 104532N (22 August 2017); https://doi.org/10.1117/12.2276313

10. Vladimir G. Krasilenko, Aleksandr I. Nikolskyy, and Alexander A. Lazarev "Designing and simulation smart multifunctional continuous logic device as a basic cell of advanced high-performance sensor systems with MIMO-structure", Proc. SPIE 9450, Photonics, Devices, and Systems VI, 94500N (6 January 2015); https://doi.org/10.1117/12.2073893

11. Vladimir G. Krasilenko, Alexander A. Lazarev, Sveta K. Grabovlyak, and Diana V. Nikitovich "Using a multi-port architecture of neural-net associative memory based on the equivalency paradigm for parallel cluster image analysis and self-learning", Proc. SPIE 8662, Intelligent Robots and Computer Vision XXX: Algorithms and Techniques, 86620S (4 February 2013); https://doi.org/10.1117/12.2003169

12. Бортник Г.Г., Васильківський М.В., Челоян В.А. Спектральний метод оцінювання джитеру в телекомунікаційних системах. - Вісник Вінницького політехнічного інституту, 2010, № 2, С. 109-114.

13. Бортник Г.Г., Васильківський М.В., Кичак В.М. Методи та засоби підвищення ефективності оцінювання фазового дрижання сигналів у телекомунікаційних системах: Монографія. - Вінниця: ВНТУ, 2015. - 140 с.

14. Бортник Г.Г., Васильківський М.В., Стальченко О.В. Пристрій аналого-цифрового перетворення високочастотних сигналів. - Вимірювальна та обчислювальна техніка в технологічних процесах.–2013, № 2.– С.82-85.

**References**

1. P. Vepakomma, T. Swedish, R. Raskar, O. Gupta, and A. Dubey, No peek: A survey of private distributed deep learning, arXiv preprint arXiv:1812.03288, 2018.

2. M. Minelli, Fully homomorphic encryption for machine learning, Ph. D. dissertation, 2018.

3. O. Gupta and R. Raskar, Distributed learning of deep neural network over multiple agents, Journal of Network and Computer Applications, vol. 116, pp. 1–8, 2018.

4. Y. Zhu, Y. Qin, Z. Zhou, X. Song, G. Liu, and W. C.-C. Chu, Digital asset management with distributed permission over blockchain and attribute-based access control, in Proc. 2018 IEEE International Conference on Services Computing (SCC). IEEE, 2018, pp. 193–200.

5. F. Hofmann, S.Wurster, E. Ron, and M. Böhmecke-Schwafert, The immutability concept of blockchains and benefits of early standardization, in Proc. 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K). IEEE, 2017, pp. 1–8.

6. Y. Zhu, Y. Qin, Z. Zhou, X. Song, G. Liu, and W. C.-C. Chu, Digital asset management with distributed permission over blockchain and attribute-based access control, in Proc. 2018 IEEE International Conference on Services Computing (SCC). IEEE, 2018, pp. 193–200.

7. Vladimir G. Krasilenko, Alexander A. Lazarev, and Diana V. Nikitovich "Modeling of biologically motivated self-learning equivalent-convolutional recurrent-multilayer neural structures (BLM_SL_EC_RMNS) for image fragments clustering and recognition", Proc. SPIE 10609, MIPPR 2017: Pattern Recognition and Computer Vision, 106091D (8 March 2018); https://doi.org/10.1117/12.2285797

8. Vladimir G. Krasilenko, Alexander A. Lazarev, and Diana V. Nikitovich "Design and simulation of optoelectronic neuron equivalentors as hardware accelerators of self-learning equivalent convolutional neural structures (SLECNS)", Proc. SPIE 10689, Neuro-inspired Photonic Computing, 106890C (21 May 2018); https://doi.org/10.1117/12.2316352

9. Vladimir G. Krasilenko, Alexander A. Lazarev, and Diana V. Nikitovich "Modeling and possible implementation of self-learning equivalence-convolutional neural structures for auto-encoding-decoding and clusterization of images", Proc. SPIE 10453, Third International Conference on Applications of Optics and Photonics, 104532N (22 August 2017); https://doi.org/10.1117/12.2276313

10. Vladimir G. Krasilenko, Aleksandr I. Nikolskyy, and Alexander A. Lazarev "Designing and simulation smart multifunctional continuous logic device as a basic cell of advanced high-performance sensor systems with MIMO-structure", Proc. SPIE 9450, Photonics, Devices, and Systems VI, 94500N (6 January 2015); https://doi.org/10.1117/12.2073893

11. Vladimir G. Krasilenko, Alexander A. Lazarev, Sveta K. Grabovlyak, and Diana V. Nikitovich "Using a multi-port architecture of neural-net associative memory based on the equivalency paradigm for parallel cluster image analysis and self-learning", Proc. SPIE 8662, Intelligent Robots and Computer Vision XXX: Algorithms and Techniques, 86620S (4 February 2013); https://doi.org/10.1117/12.2003169

12. Bortnyk G.G., Vasylkivskyi M.V., Cheloyan V.A. Spektral′nyy metod otsinyuvannya dzhyteru v telekomunikatsiynykh systemakh. - Visnyk Vinnyts′koho politekhnichnoho instytutu, 2010, № 2, S. 109-114.

13. Bortnyk G.G., Vasylkivskyi M.V., Kychak V.M. Metody ta zasoby pidvyshchennya efektyvnosti otsinyuvannya fazovoho dryzhannya syhnaliv u telekomunikatsiynykh systemakh: Monohrafiya. - Vinnytsya: VNTU, 2015. - 140 s.

14. Bortnyk G.G., Vasylkivskyi M.V., Stalchenko O.V. Device for analog-digital conversion of high-frequency signals. - Measuring and computing equipment in technological processes.–2013, No. 2.– P.82-85.