

Парадигми управління ідентифікаційними даними у світлі розвитку пристроїв IoT та штучного інтелекту

Костенко О. В.

*доктор філософії (Ph.D.) з юридичних наук,
завідувач наукової лабораторії теорії цифрової трансформації
і права наукового центру цифрової трансформації і права
Державна наукова установа «Інститут інформації, безпеки і права
Національної академії правових наук України»
вул. Пилипа Орлика, Київ, Україна,
orcid.org/0000-0002-2131-0281
antizuk@gmail.com*

Ключові слова: парадигма, управління ідентифікаційними даними, ідентифікація, атрибут, штучний інтелект.

У роботі досліджено питання класифікації парадигм управління ідентифікаційними даними. Сьогодні процеси управління ідентифікаційними даними в інформаційно-комунікаційних системах і мережі Інтернет є вкрай актуальними. Запропоновано на основі узагальнюючих даних щодо сучасних технічних і юридичних механізмів і процедур ідентифікації суб'єктів та об'єктів застосувати нову парадигму управління ідентифікаційними даними.

Автор акцентує на необхідності розробки та створення єдиних підходів правової регуляції у сфері управління ідентифікаційними даними.

На нашу думку, розвиток технологій Інтернету речей і штучного інтелекту дозволяє сформулювати нову, четверту парадигму управління ідентифікаційними даними.

Запропоновано сучасну транскордонну трирівневу суб'єктно-об'єктову парадигму, котра об'єднує суб'єктно-об'єктовий рівень, рівень доступу/запиту на ідентифікаційні дані та третю незалежну сторону, що здійснює процедури верифікації транзакцій і забезпечує гарантії достовірності ідентифікаційних даних, які застосовуються у цих транзакціях. Парадигма базується на генеральній ідеї, котра полягає в тому, що управління ідентифікаційними даними вважатимуться процеси, функції та процедури отримання, перевірки, реєстрації, збереження, використання, захисту, знищення ідентифікаційних даних суб'єктів та об'єктів у процесах їх взаємодії. Суб'єктами сфери управління ідентифікаційними даними будуть виступати не тільки фізичні та юридичні особи або представники юридичної особи, але й об'єкти сфери управління ідентифікаційними даними – системи зі штучним інтелектом і пристрої IoT.

Транскордонна трирівнева суб'єктно-об'єктова парадигма управління ідентифікаційними даними дозволить вирішити значну частину проблем, пов'язаних із технічним, техніко-юридичним і правовим регулюванням у сфері управління ідентифікаційними даними. Створення простору довіри у зазначеній сфері позитивно вплине на зростання рівня застосування електронних сервісів у всіх сферах життєдіяльності суспільства.

Paradigms of management of identification data in the light of development of IoT devices and artificial intelligence

Kostenko O. V.

Doctor of Philosophy (Ph.D.) in Law,

*Head of the Scientific Laboratory of Digital Transformation Theory and Law of the
Scientific Center for Digital Transformation and Law*

*The State Scientific Institution of the Institute of Information, Security and Law of the
National Academy of Legal Sciences of Ukraine*

Pylyp Orlyk str., 3, Kyiv, Ukraine

orcid.org/0000-0002-2131-0281

antizuk@gmail.com

Key words: *paradigm,
identification data
management, identification,
attribute, artificial
intelligence.*

The paper investigates the classification of identification data management paradigms. Today, the processes of identity management in information and communication systems and the Internet are extremely relevant. It is proposed to apply a new paradigm of identification data management on the basis of generalized data on modern technical and legal mechanisms and procedures of identification of subjects and objects. In our opinion, the development of Internet of Things technologies and artificial intelligence allows us to form a new, fourth paradigm of identity data management. object-level, access / request for credentials, and an independent third party that performs transaction verification procedures and ensures that the credentials used in those transactions are accurate. The paradigm is based on the general idea that the management of credentials will be the processes, functions and procedures for obtaining, verifying, registering, storing, using, protecting, destroying the credentials of subjects and objects in the processes of their interaction. In turn, the subjects of the sphere of identification data management will be not only natural and legal persons or representatives of the legal entity, but also objects of the sphere of identification data management – systems with artificial intelligence and IoT devices. The subject-object paradigm of identification data management will allow solving a significant part of the problems related to technical, technical-legal and legal regulation in the field of identification data management. Creating a space of trust in the field of identity management will have a positive impact on the growth of the use of electronic services in all spheres of society.

Вступ. Науково-технічна революція 4.0. дала поштовх стрімкому прискоренню впровадження цифрових технологій практично в усі напрями життєдіяльності людства. Крім того, ситуація із пандемією коронавірусної хвороби (COVID-19) стимулювала цифровізацію навіть таких консервативних сфер, як медицина, адвокатура, релігія тощо.

Постановка проблеми. Проблематикою управління ідентифікаційними даними займаються багато дослідників, серед яких І. Карретеро, Г. Іск'єрдо-Морено, М. Василе-Кабесасі, Л. Буссард, Е. Ді Нітто, О. Нано, А. Йосанг, С. Поуп, Е. Малікі, Дж.М. Сейньор, А. Перес-Мендес, Д. Чадвік, С. Клаус, М. Контопп, В. Кумар,

С. Бузефран та ін. Водночас серед вітчизняних наукових організацій проблеми сфери управління ідентифікаційними даними раніше не порушувалися, а аналогічні дослідження українськими науковцями не здійснювалися.

Управління ідентифікаційними даними у цифровому світі не має чітко визначеного значення, однак технологічне управління ідентифікацією в її найширшому розумінні належить до адміністрування та характеристик ідентифікаційних атрибутів, управління процесами ідентифікації та використання ідентифікаційних даних. Правове регулювання управління ідентифікаційними даними містить достатньо законодавчих проблем, які стосуються не тільки інформаційної, а й інших галузей права.

Метою роботи є дослідження сучасних парадигм у сфері управління ідентифікаційними даними, а також теоретичне обґрунтування та наукова розробка пропозицій створення більш сучасної парадигми, що містить такі напрями, як пристрої Інтернету речей (IoT) і штучний інтелект і їх транскордонне застосування.

Виклад основного матеріалу дослідження.

Розвиток технологій сягнув такого етапу, що створення, розповсюдження, використання та зберігання інформації у цифровій формі потребує конкретних споживачів – суб'єктів або об'єктів. Суб'єктами виступають фізичні та юридичні особи, а об'єктами необхідно вважати сучасні пристрої Інтернету речей (IoT) та пристрої або програми зі штучним інтелектом. Об'єктів і суб'єктів об'єднує одне – специфічні та притаманні їм одним атрибути або набір атрибутів, які прийнято називати комплексним поняттям «ідентифікаційні дані».

Саме ідентифікаційні дані є «золотим ресурсом», за допомогою якого інформаційні дані перетворюються на споживчий продукт. Державні установи, приватні компанії й організації розробляють і впроваджують безліч технічних схем ідентифікації й управління ідентифікаційними даними, які досі не мають технологічної сумісності технічних рішень під час використання ідентифікаційних даних, не здатні взаємодіяти між собою і не піддаються правовому регулюванню.

Створення нових суспільних відносин у сфері управління ідентифікаційними даними потребує

своєчасного та швидкого реагування законодавства держави. Актуальними є проблеми формування понятійно-категоріального апарату у сфері управління ідентифікаційними даними та розробки і впровадження єдиної парадигми управління ідентифікаційними даними як у межах національних правових доктрин, так і у транскордонному режимі.

Історично зміни наукових парадигм відбуваються у період науково-технічної революції, тож саме сьогодні створені умови для формування сучасної парадигми управління ідентифікаційними даними. Формування будь-якої парадигми неможливе без чіткого формування компонентів, які визначають подальші практичні, теоретичні та методологічні принципи побудови світу нової цифрової формації. Ключовими компонентами вважатимуться: ідентифікаційні дані суб'єктів та об'єктів, управління ідентифікаційними даними. Сьогодні немає єдиної сталої думки, що саме вважати ідентифікаційними даними й управлінням ідентифікаційними даними.

Це відображено у намаганні створити єдині та прийнятні для всіх дефініції. Так, проблеми сучасного понятійно-категоріального апарату в українському законодавстві відображені автором у науковому дослідженні «Управління ідентифікаційними даними (ідентифікація): проблеми понятійно-категоріального апарату». Генезис визначення «управління ідентифікаційними даними» розглянуто у роботах Вікаса Кумара [1] та відображено у таблиці 1.

Таблиця 1

Визначення поняття «управління ідентифікаційними даними або управління ідентифікацією»

Рік	Визначення
1	2
2001	Система управління ідентифікацією надає інструменти для управління всіма частковими ідентичностями людини у цифровому світі. Часткова ідентичність може або не може однозначно ідентифікувати особу. Наприклад, людина може використовувати одну або кілька ідентифікаційних даних особи [2].
2003	Управління ідентичністю – це набір бізнес-процесів і допоміжної інфраструктури для створення, підтримки та використання цифрових ідентичностей [3].
2004	Управління ідентифікацією та доступом стосується процесів, технологій і політики управління цифровими посвідченнями. Це також стосується контролю осіб за доступом до ресурсів [4].
2007	Управління ідентифікацією надає засоби для управління та вибіркового розкриття інформації про особу, що стосується користувачів організації та забезпечення потреб у конфіденційності [5].
2008	Управління ідентифікацією зазвичай називають сукупністю процесів та інструментів, які служать для встановлення ідентичності особи користувача як працівника, замовника, підрядника тощо у системі [6].
2008	Управління ідентифікацією дозволяє керувати особистістю людей у двох різних сенсах, тобто керує людиною у фізичних просторах. Крім того, це дозволяє зберігати складні цифрові образи людей у різних базах даних [7].
2008	Системи управління ідентифікацією використовуються для управління ідентифікаційними даними користувачів у декількох системах і забезпечення способу доступу користувачів до ресурсів організації. Це робиться протягом усього життєвого циклу користувача в організації за допомогою єдиного входу і перевірки облікових даних користувача [8].

Продовження таблиці 1

1	2
2009	Управління особистими даними – це набір функцій і можливостей для адміністрування, управління, обслуговування, виявлення, обміну інформацією, забезпечення політики й автентифікації. Це використовується для забезпечення інформації про особу та безпеки. Воно надає інструменти для управління індивідуальними ідентичностями у цифровому середовищі [9].
2009	Управління особистістю використовується для захисту даних користувачів, що стосуються місцезнаходження, інтересів тощо. Це робиться у цифровому світі так, як це роблять у фізичному світі самі користувачі [10].
2011	Управління ідентичністю є моделлю, яка забезпечує потрібну кількість можливостей у потрібний час [11].
2017	Управління особистістю – це поєднання бізнес-процесів і технологій, що використовуються для управління даними в ІТ-системах. Програми керують даними для користувацьких об'єктів, атрибутів, прав безпеки та факторів автентифікації [12].
2017	Управління особистістю – це широка адміністративна сфера, яка займається ідентифікацією осіб у такій системі, як країна, мережа чи організація. Це контролює їх доступ до ресурсів у цій системі, асоціюючи права користувачів та обмеження зі встановленою особистістю [13].

Проблемою, котра впливає із попередньої, є генерація сучасних парадигм сфери управління ідентифікаційних даних.

Науковці формують парадигми, спираючись на базові визначення складників ідентифікаційних процесів, механізми забезпечення застосування й обробки ідентифікаційних даних, алгоритми та технології, які запроваджуються в окремих галузях і сферах життєдіяльності суспільства. Так, пропонуються три парадигми управління ідентифікаційними даними:

– **мережева центрична**, що формується на базі локального (корпоративного) центру обробки ідентифікаційних даних;

– **сервісна центрична**, яка формується з різних і незалежних центрів обробки ідентифікаційних даних, у котрих один і той самий суб'єкт або об'єкт може мати різні ідентифікаційні атрибути ідентифікаційних даних;

– **суб'єктно-об'єктова**, у якій атрибути ідентифікаційних даних для процедур ідентифікації розміщуються на засобах, котрими безпосередньо володіє суб'єкт, або невід'ємно належать суб'єкту.

На нашу думку, розвиток технологій Інтернету речей і штучного інтелекту дозволяє сформуванню нової, четвертої парадигми управління ідентифікаційними даними – транскордонну трирівневу суб'єктно-об'єктову парадигму.

Транскордонна трирівнева суб'єктно-об'єктова парадигма об'єднує суб'єктно-об'єктовий рівень, рівень доступу/запиту на ідентифікаційні дані та третю незалежну сторону, котра здійснює процедури верифікації транзакцій між першим і другим рівнем, а також надає гарантії достовірності ідентифікаційних даних, що застосовуються у цих транзакціях. Парадигма базується на генеральній ідеї, яка полягає у тому, що управлінням ідентифікаційними даними вважатимуться процеси, функції та нормативно-правові акти, які регулюють

процедури отримання, перевірки, реєстрації, збереження, використання, захисту, знищення ідентифікаційних даних суб'єктів та об'єктів. У свою чергу, суб'єктами сфери управління ідентифікаційними даними виступатимуть не тільки фізичні та юридичні особи або представники юридичної особи, але й об'єкти сфери управління ідентифікаційними даними – системи зі штучним інтелектом і пристрої IoT [14].

Третя незалежна сторона призначена забезпечити процедури надійності та достовірності наданих до системи ідентифікаційних даних, їх автентичність і юридичну відповідність об'єкту та суб'єкту володільців даних, а також забезпечити страхові гарантії та юридичну значимість транзакцій [15].

Фактично управління ідентифікаційними даними може здійснюватися за волею суб'єктів і функціональним призначенням об'єктів за моделями, побудованими відповідно до будь-якої із трьох парадигм, наприклад, **ізолюваною, централізованою або федеративною моделлю**.

Водночас застосування нових моделей на основі транскордонної трирівневої суб'єктно-об'єктової парадигми сприятиме формуванню транскордонного простору довіри та передбачає впровадження на національному рівні додаткових суб'єктів – приватних або державних довірчих центрів, які забезпечать надійні процедури ідентифікації й управління ідентифікаційними даними у приватному та державному секторі електронних послуг і транзакцій.

За даними Міністерства цифрової трансформації України, в нашій державі налічуються і функціонують понад 350 державних реєстрів, що мають часто архаїчну структуру Excel-таблиць або Google-документів, а інформація, яка міститься в них, дублюється або взагалі не оновлюється, інтелектуальна і юридична власність перебуває у третіх осіб. Також не існує єдиного

нормативного регулювання правил і стандартів для створення та функціонування держреєстрів, що робить реєстри не інтероперабельними та мало захищеними від зовнішнього втручання та внутрішнього несанкціонованого коригування.

Сьогодні Україною обрано шлях створення системи обміну даними між наявними реєстрами та побудови системи уніфікації для створення нових реєстрів даних. Безперечно, це позитивний напрям [16], однак, на нашу думку, така схема управління реєстрами містить ризики, які полягають у тому, що ідентифікаційні дані суб'єктів та об'єктів все одно будуть розміщуватися одночасно у різних реєстрах різних власників реєстрів. У цьому разі доцільно на основі транскордонної трирівневої суб'єктно-об'єктової парадигми розробити один єдиний реєстр ідентифікаційних даних фізичних і юридичних осіб, а також ідентифікаційні дані пристроїв IoT та штучного інтелекту. Інші реєстри не повинні містити ідентифікаційні дані й автоматично взаємодіяти

із реєстром управління ідентифікаційними даними за допомогою кодів доступу. Верифікацію транзакцій доцільно покласти на третю довірчу сторону, котра забезпечить транскордонний режим електронних послуг, страхування транзакцій і їх юридичний супровід.

Висновки. Парадигми управління ідентифікаційними даними спрямовують дослідників на створення різних моделей управління ідентифікаційними даними, однак не враховуються сучасні досягнення у сфері штучного інтелекту та пристроїв Інтернету речей. Запропонована транскордонна трирівнева суб'єктно-об'єктова парадигма управління ідентифікаційними даними дозволить вирішити значну частину проблем, пов'язаних із технічним, техніко-юридичним і правовим регулюванням у сфері управління ідентифікаційними даними, що сприятиме створенню простору довіри у цій сфері та формуванню транскордонного простору довіри, а також позитивно вплине на зростання рівня довіри до електронних сервісів у всіх сферах життєдіяльності суспільства.

Література

1. Kumar V. Identity Management Systems: A Comparative Analysis. *International Journal of Strategic Decision Sciences*. 2018. DOI: 10.4018/IJSDS.2018010105
2. Clauß, S., Köhntopp M. Identity management and its support of multilateral security. *Computer Networks*. № 37 (2). 2001. P. 205–219. DOI: 10.1016/S1389-1286(01)00217-1
3. Manders-Huits, N., Van den Hoven, J. Moral identification in identity management systems. In *The future of identity in the information society*. 2008. P. 77–91. DOI: 10.1007/978-0-387-79026-8_6
4. Chog F. Chonka A., Xiang Y., Zhou W. Microsoft Corporation, Architecture Journal. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications*. 2001. P. 1097–1107. URL: <https://www.researchgate.net/file.PostFileLoader.html?id=4fcf6e52e39d5e911e000000&assetKey=AS%3A271742583410689%401441799888783> (дата звернення: 20.02.2021)
5. Del Álamo J. Leveraging New Business Models with Identity Management—An e-learning case study. 2007. URL: https://www.cs.kau.se/IFIP-summer-school/summer-school2009/IFIP2007POST/papers/S11_P2_Jose%20Alamo.pdf (дата звернення: 20.02.2021)
6. De Hert P. Identity management of e-ID, privacy and security in Europe. *Information Security Technical Report*. 2008. № 13 (2). P. 71–75. DOI: 10.1016/j.istr.2008.07.001 (дата звернення: 18.08.2021)
7. Hewitt, A., Forte, A. Crossing boundaries: Identity management and student/faculty relationships on the Facebook. Poster presented at CSCW, Banff, Alberta. 2008. URL: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.94.8152> (дата звернення: 18.08.2021)
8. Tracy K. Identity management systems. *Journals & Magazines IEEE Potentials*. № 27 (6). 2008. P. 34–37. DOI: 10.1109/MPOT.2008.929295 (дата звернення: 18.08.2021)
9. Chadwick D. Federated identity management. *Foundations of security analysis and design*. 2009. P. 96–120. URL: <https://kar.kent.ac.uk/30609/1/FederatedIdManChapter.pdf> (дата звернення: 18.08.2021)
10. Tatli E., Lucks S. Mobile identity management revisited. *Electronic Notes in Theoretical Computer Science*. 2009. P. 125–137. DOI: 10.1016/j.entcs.2009.07.044
11. Olden E. Architecting a cloud-scale identity fabric. *Computer*. № 44 (3). 2011. P. 52–59. DOI: 10.1109/MC.2011.60
12. IDG Communication. Marketing services. 2017. URL: <https://www.idg.com/marketingservices/> (дата звернення: 18.08.2021)
13. Techtargget.com. Search Unified Communication. 2017. URL: <http://searchunifiedcommunications.techtargget.com/> (дата звернення: 18.08.2021)
14. Kostenko O. Identification data management: legal regulation and classification. *Scientific Journal of Polonia University. Periodyk Naukowy Akademii Polonijnej*. № 6/2020. P. 198–204. DOI:10.23856/4325

15. Костенко О.В. Електронні довірчі послуги: правовий аспект транскордонного використання : монографія. Київ – Одеса, 2020. 167 с.
16. Федоров М. Корупція в держреєстрах: як її подолати. *Українська правда*. 2021. URL: <https://www.epravda.com.ua/columns/2021/08/5/676592/> (дата звернення: 18.08.2021)

References

1. Kumar V. Identity Management Systems: A Comparative Analysis. *International Journal of Strategic Decision Sciences*. 2018. DOI: 10.4018/IJSDS.2018010105
2. Clauß, S., Köhntopp M. Identity management and its support of multilateral security. *Computer Networks*, 37 (2). 2001. 205–219p. DOI: 10.1016/S1389-1286(01)00217-1
3. Manders-Huits, N., Van den Hoven, J. Moral identification in identity mangement systems. In *The future of identity in the information society*. 2008. 77–91p. DOI: 10.1007/978-0-387-79026-8_6
4. Chog F. Chonka A., Xiang Y., Zhou W. Microsoft Corporation, *Architecture Journal*. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. *Journal of Network and Computer Applications*. 2001. 1097–1107p. URL: <https://www.researchgate.net/file.PostFileLoader.html?id=4fcf6e52e39d5e911e000000&assetKey=AS%3A271742583410689%401441799888783>
5. Del Álamo J. Leveraging New Business Models with Identity Management–An e-learning case study. 2007. URL: https://www.cs.kau.se/IFIP-summerhschool/summerhschool2009/IFIP2007POST/papers/S11_P2_Jose%20Alamo.pdf
6. De Hert P. Identity management of e-ID, privacy and security in Europe. *Information Security Technical Report*. 2008. 13 (2). 71–75p. DOI: 10.1016/j.istr.2008.07.001
7. Hewitt, A., Forte, A. (2008). Crossing boundaries: Identity management and student/faculty relationships on the Facebook. Poster presented at CSCW, Banff, Alberta. URL: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.94.8152>
8. Tracy K. (2008). Identity management systems. *Journals & Magazines IEEE Potentials*. 27 (6). 34–37 p. DOI: 10.1109/MPOT.2008.929295
9. Chadwick D. (2009). Federated identity management. In *Foundations of security analysis and design*. 96–120p. URL: <https://kar.kent.ac.uk/30609/1/FederatedIdManChapter.pdf>
10. Tatli E., Lucks S. (2009) Mobile identity management revisited. *Electronic Notes in Theoretical Computer Science*. 2009. 125–137 p. DOI:10.1016/j.entcs.07.044
11. Olden E. (2011) Architecting a cloud-scale identity fabric. *Computer*, 44(3).52–59 p. DOI: 10.1109/MC.2011.60
12. IDG Communication. Marketing services. (2017). URL: <https://www.idg.com/marketingservices/>
13. Techtarger.com. Search Unified Communication. (2017). URL: <http://searchunifiedcommunications.techtarger.com/>
14. Kostenko O. (2020). Identification data management: legal regulation and classification. / *PNAP. Scientific Journal of Polonia University Peridyk Naukowy Akademii Polonijnej*. № 6/2020. 198–204 p. DOI: 10.23856/4325
15. Kostenko O. (2020). Elektronni dovirchi posluy: pravovyj aspekt transkordonnogo vykorystannya: monografiya. Kyyyiv – Odesa.
16. Fedorov M. (2021). Koruptsiia v derzhreiestrakh: yak yii podolaty [Corruption in state registers: how to overcome it]. *Ukrainska pravda (electronic journal)*, 2021. URL: <https://www.epravda.com.ua/columns/2021/08/5/676592/> (accessed 20 august January 2021).