УДК 342.951(004.896)
DOI https://doi.org/10.32837/chern.v0i1.177

О. В. Костенко
доктор філософії (Ph.D.) в галузі права,
в. о. завідувача науково-дослідної лабораторії теорії і права цифрових трансформацій
Науково-дослідного центру цифрових трансформацій і права
Науково-дослідного інституту інформатики і права
Національної академії правових наук України
orcid.org/0000-0002-2131-0281

ІДЕНТИФІКАЦІЯ IOT: ВИТОКИ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ УПРАВЛІННЯ ІДЕНТИФІКАЦІЙНИМИ ДАНИМИ

У роботі досліджується питання розробки механізмів правового забезпечення управління ідентифікаційними даними пристроїв IoT. Аналізуються сучасні технічні та юридичні механізми і процедури ідентифікації суб'єктів та об'єктів. Запропоновано застосувати як приклад мережеву модель OSI для класифікації елементів мережі пристроїв IoT за функціональними ознаками. Також здійснено огляд різновидів сучасних технологій, що використовуються для забезпечення функціонування екосистем пристроїв IoT, а саме: радіотехнології, різних універсальних ідентифікаційних систем, технічних стандартів, рішень, що забезпечують безпеку даних, та платформи сумісності пристроїв IoT, а також напрями розвитку технологій ідентифікації та управління ідентифікаційними даними відомих розробників.

Проаналізовано стан національного законодавства, що регулює правовідносини у сфері управління ідентифікаційними даними. Підкреслено, що Україна має певний позитивний досвід в напрямі технічної організації та розвитку процесів електронної ідентифікації та правову основу з метою формування сучасного законодавства у сфері управління ідентифікаційними даними. Водночас вказано на низку характерних недоліків, пов'язаних із ситуативною, малосистемною і неструктурованою модернізацією національного законодавства, насиченням його незбалансованою в юридичному та нормопроєктувальному сенсі термінологією.

Автором запропоновано сучасне рішення, яке полягає у створенні системи технічних стандартів, юридичних правил та норм, порядків і процедур перевірки ідентифікаційних даних. Дане рішення, як багаторівнева соціотехніча система, забезпечить тотожність ідентифікаційних даних з фізичною або юридичною особою, пристроєм або цифровим об'єктом для взаємодії із цифровою екосистемою. Модернізація нормативно-правової бази, яка здійснює регулювання суспільних відносин у сфері управління ідентифікаційними даними, спрямована на визначення та формування суб'єктів та об'єктів цієї сфери, їх прав та обов'язків, а також формування видів правопорушень та відповідальності за їх скоєння. Відповідно, не омине осучаснення і діючих правових норм чинного законодавства України.

Ключові слова: пристрої IoT, ідентифікаційні системи, управління ідентифікаційними даними, ідентифікація, ідентифікаційні дані, технічні стандарти, штучний інтелект, електронні довірчі послуги.

Kostenko O. V. **IOT IDENTIFICATION: ORIGINS OF THE PROBLEM OF LEGAL REGULATION OF IDENTIFICATION DATA MANAGEMENT**

The question of development of mechanisms of the legal providing of management identification data of devices of IoT is in-process investigated.

Modern technical and legal mechanisms and procedures of authentication of subjects and objects are analysed. It is suggested to apply as an example the network model of OSI for classification of elements of network of devices of IoT on functional signs. The review of varieties of modern technologies that is used for providing of functioning of ecosystems of devices of IoT is also carried out, namely: radiotechnology, different universal identification systems, technical standards, decisions, that provide safety of data and platform of compatibility of devices of IoT, and also directions of development of technologies of authentication and management of identification data of known.

The state of national legislation that regulates legal relationships in the field of the management of identification data is analysed. Underline, that Ukraine has positive experience is certain in direction of technical organization and development of processes of electronic authentication and legal framework is stopped up with the aim of forming of modern legislation in the field of the management of identification data. At the same time, it is indicated on the row of the characteristic defects, related to situation, littlesystem and unstructured modernisation of national legislation, satiation of him not balanced in legal sense

An author is offer modern solution that consists in creation of the system of technical standards, legal rules and norms, orders and procedures of identification background check. This decision, as a multilevel соціотехніча system, will provide equality of identification data with a physical or legal person, device or digital object for co-operating with a digital ecosystem. Modernisation of normatively-legal base, that carries out adjusting of public relations in the field of the management of identification data, is sent to determination and forming of subjects and objects of this sphere, their rights and duties, and also forming of types of offences and responsibility for their feasance. Accordingly will not go round осучаснення and operating legal norms of current legislation

Key words: devices of IoT, identification systems, management of identification data, authentication, identification data, technical standards, artificial intelligence, electronic confidence services.

Постановка проблеми. Сучасне суспільство увійшло в епоху новітньої науково-технічної революції та економічної глобалізації. Сьогодні однією з її рушійних сил є інформаційно-комунікаційні технології. Так, одним із ключових елементів технологій передачі інформації є дані, за якими

можливо ідентифікувати суб'єктів та об'єктів за притаманні їм ідентифікаційні атрибути, тобто здійснювати процеси управління ідентифікаційними даними, в тому числі і пристроями IoT.

Вирішення проблеми управління процесами застосування цифрових ідентифікаційних даних є основою для сучасного розвитку електронної економіки та торгівлі. Нині в Україні здійснюються певні заходи в напрямі організації та розвитку електронної ідентифікації, які спрямовані на виключно технічні способи ідентифікації. З огляду на це спрямування юридичних зусиль в напрямі вирішення проблеми управління ідентифікаційними даними пристроїв IoT є вкрай актуальним завданням.

Метою статті є дослідження правового забезпечення управління ідентифікаційними даними пристроїв IoT, а саме правових механізмів процедури ідентифікації суб'єктів та об'єктів, з метою теоретичного обґрунтування та наукової розробки пропозицій удосконалення національного законодавства.

Результати аналізу наукових публікацій. Питання правового регулювання суспільних відносин, що пов'язано з використанням окремих видів ідентифікаційних даних (персональні дані, пристрої Інтернету речей, системи управління інформаційною безпекою (СУІБ), штучний інтелект, електронні довірчі послуги, квантова криптографія, електронний цифровий підпис) досліджували і досліджують такі українські вчені: О.А. Баранов, В.М. Брижко, В.Б. Вєхова, І.Д. Горбенко, В.Я.Тацій, В.Г. Пилипчук, О.В. Потій, О.В. Різник, Н.А. Савінова, М.В. Крачевський, О.Е. Радутний. Крім того, науковцями багатьох міжурядових груп, приватних міжнародних груп і комерційних структур активно вивчається питання управління ідентифікаційними даними і наявні в цій галузі можливості, розробляються технічні стандарти і процедури, а також здійснюється пошук шляхів реалізації життєздатних систем ідентифікації. Водночас звертає на себе увагу недостатність теоретичних напрацювань з питання, що досліджується, а також відсутності комплексних наукових досліджень з правового забезпечення управління ідентифікаційними даними пристроїв IoT.

Виклад основних положень. Неспростовним фактом є те, що людство вступило в епоху новітньої науково-технічної революції та економічної глобалізації. Масштабність, швидкість та багатовекторність розвитку науки і техніки надзвичайно ефективно впливають на правові, економічні, політичні, духовні та інші суспільні відносини, створюючи їх нові різновиди. Так, однією із рушійних сил нової науково-технічної революції нині є розвиток інформаційно-комунікаційних технологій. Це сприяло впровадженню інформаційних технологій передачі даних та використанню інформації в цифровому виді практично у всіх сферах суспільного життя, а саме: традиційні текстові і графічні дані, мультимедійні формати (фото-, аудіо-, відеодані) тощо, що транслюються різноманітними способами мережею Інтернет та іншими комунікаційними засобами та системами.

Одним із ключових елементів технологій та систем передачі даних є наявність інформації, за якою можливо ідентифікувати суб'єктів та об'єктів за притаманні їм ідентифікаційні атрибути – ідентифікаційні дані.

Ідентифікаційними даними вважається інформація про конкретного суб'єкта в формі одного або декількох атрибутів, що дозволяють суб'єкту бути достатньою мірою відмінним у певному контексті, або набір атрибутів особи, які дозволяють цій особі відрізнятися від інших осіб у конкретному контексті, а саме е-екосистемі IoT.

Водночас управлінням ідентифікаційними даними в широкому сенсі прийнято вважати набір прийомів, що дозволяють управляти процесами ідентифікації, автентифікації і авторизації фізичних і юридичних осіб, пристроїв IoT в режимі онлайн з метою отримання електронних сервісів та даних.

Сучасний IoT являє собою локальні об'єднання автономних мікроелектромеханічних систем (MEMS), радіотехнологій передачі даних, програмних продуктів, електронних сервісів, Інтернету та галузевих або соціальних інформаційно-комунікаційних хабів (е-екосистем). Структурно IoT умовно можна поділили на елементи за принципом мережевої моделі OSI (The Open Systems Interconnection model). До першого рівня моделі (media layers) належать фізичний, мережевий та рівень додатків, тобто безпосередньо IoT пристрої, радіотранспортна мережа та мережеве обладнання, протоколи передачі даних та інтерфейси, модулі та алгоритми ідентифікації. До другого рівня (host layers) доцільно віднести модулі управління, аналітики та зберігання даних, Інтернет-комунікації, програмні платформи, хаби.

На рівні Media layers протоколами передачі даних пристроїв IoT вважаються набір правил, що створює єдиний технологічний простір передачі даних та визначає загальні алгоритми взаємодії між об'єктами мережі Інтернету речей за допомогою програм, мережевих вузлів чи систем. Так, зараз у мережі IoT на заміну всім відомому протоколу HTTP прийшли сучасні протоколи для наступних ділянок: сенсор-сенсор (DDS), сенсор-сервер (CoAP, XMPP, MQTT, STOMP), сервер-сервер (AMQP) [1].

Для передачі даних пристроїв IoT застосовують такі радіотехнології, як LoRaWan, LTE-M, Sigfox, NB-IoT, NFC BLE, Wi-Fi, Z-Wave, ZigBee. Одні, такі як Zigbee, BLE, WiFi, мають малу

дальність дії, інші, як 3G і LTE, мають проблеми енергоспоживання і нестабільний радіус або сектор радіопокриття [2].

До відомих платформ IoT належать: Amazon Web Services, Microsoft Azure, ThingWorx IoT Platform, IBM's Watson, Cisco IoT Cloud Connect, Salesforce IoT Cloud, Oracle Integrated Cloud, GE Predix [3].

Ідентифікатори стандарту IoT сьогодні прийнято розділяти на такі категорії: Ідентифікатори об'єктів, які використовуються для ідентифікації фізичних або віртуальних об'єктів (URIs, URL); Ідентифікатори зв'язку, які застосовуються для унікальної ідентифікації пристроїв у межах комунікації з іншими пристроями, включаючи Інтернет-зв'язок (IPv4, IPv6, E.164); Ідентифікатори додатків, які визначають унікальні програми, що використовуються в межах IoT додатків (EPC, UPC, Handle/DOI, UUID, MAC, URI, URL, Ecode, OID, CID) [4].

Нині в світі існують різні універсальні ідентифікаційні системи, такі як Object IDentifier (OID), електронний код продукту (EPC), універсально унікальний ідентифікатор IDentifier (UUID) і міжнародний ідентифікатор мобільного обладнання Identity (IMEI) тощо.

Сучасне IoT середовище неоднорідне і в механізмах ідентифікації. Це наслідки не стільки значної кількістю пристроїв, скільки різноманітності унікальних схем ідентифікації (ISS) або оригінальних методів ідентифікації різних виробників, що стає бар'єром обміну даними між неспорідненими хабами, додатками або платформами. Найбільш поширеними схемами ідентифікації є OID, EPC та UUID.

OID – широко використовуваний механізм ідентифікації, спільно розроблений ITU-T (Міжнародний сектор телекомунікаційної стандартизації телекомунікацій) і ISO/IEC (Міжнародна організація зі стандартизації / Міжнародної електротехнічної комісії), призначений для встановлення унікального та стійкого в часі реквізиту об'єкта або пристрою, за яким буде здійснюватися його ідентифікація [5].

EPC – універсальний ідентифікатор будь-якого фізичного об'єкту, унікальний серед усіх існуючих об'єктів. Ідентифікатор EPC дозволяє контролювати розташування об'єктів в інформаційних системах, що входять до мережі EPCglobal. [6].

UUID – це 128-розрядне число, яке використовується для унікальної ідентифікації сутності або об'єкта в просторі та часі, або стандарт ідентифікації, який використовується під час створення програмного забезпечення, затверджений Open Software Foundation (OSF) як частина розподіленого комп'ютерного середовища (DCE) [7].

Різноманітність підходів ідентифікації торкнулась і технічних стандартів, рішень безпеки та платформ сумісності IoT, які розроблюють багато організацій і галузевих груп. Існує декілька популярних стандартів і платформ для надання послуг IoT, таких як «oneM2M», «GS1», «OCF» та «FIWARE».

Так, в 2012 році проєкт oneM2M заснували вісім провідних світових організацій інформаційно-комунікаційних технологій (ІКТ). Основною метою oneM2M є визначення комплексної платформи M2M для надання послуг з взаємодії в організації та між організаціями. Архітектура oneM2M походить від багаторівневого підходу, при якому кожен рівень відповідає за певний набір дій: рівень програм, загальний рівень послуг і мережевий рівень [8].

Проєкт GS1 як некомерційну організацію створено в 1973 році Uniform Code Council, Inc. (UCC), відомий зараз як GS1 US. Метою проєкту є розробка стандартів, таких як штрих-коди та RFID. Стандарти ідентифікації GS1 надають ключі ідентифікації GS1, які є унікальними ідентифікаторами для позначення реальних суб'єктів або об'єктів. Комбінована система стандартів GS1 відіграє важливу роль у підключенні пристроїв на базі IoT. GS1 виконує вимогу ідентифікації об'єктів за допомогою ключів ідентифікації GS1 [9].

Проєкт OCF – це галузева група, яка спрямована на впровадження рекомендацій щодо сумісності та стандартів специфікації для пристроїв IoT. OCF є однією з найбільших організацій промислової стандартизації IoT і має більш ніж 300 компаній-членів. За проєктом створено набір специфікацій, референційне впровадження та сертифікація для пристроїв на базі IoT, з метою забезпечення сумісності та створення загальної моделі даних для взаємодії пристроїв IoT [10].

Проєкт FIWARE ініційований Європейською Комісією в рамках державно-приватного партнерства Future Internet і був започаткований 3 травня 2011 року спільно з основними партнерами з інформаційно-комунікаційних технологій та компаніями Європи. Основна мета FIWARE є надання майбутніх інтернет-послуг і додатків із використанням універсальних ідентифікаторів. FIWARE використовує специфікацію інтерфейсу служби Open Mobile Alliance Next Generation (OMA NGSI) для обміну інформацією та керування даними. Проєкт підтримується грантом Інституту інформаційно-комунікаційних технологій, що фінансується Корейським урядом [11].

Окремо слід звернути увагу на нові проекти альянсів – FIDO та AIOTI.

Альянс з інновацій Інтернет речей AIOTI (The Alliance for Internet of Things Innovation) створено у 2015 році з ініціативи Єврокомісії. Мета альянсу – розвиток та підтримка діалогу й взаємодії між різними країнами Європейського Союзу, які прогнозують прогрес IoT у власних економіках [12; 13].

Проєкт FIDO Alliance (Fast IDentity Online). Альянс засновано у 2013 році компаніями Agnitio, Infineon Technologies, Lenovo, Nok Nok Labs, PayPal та Validity. Згодом до них приєдналися Google, Microsoft, Samsung, Yubico та NXP. Метою Альянсу є створення стандартизованого підходу до автентифікації в Інтернеті та випуску відповідних пристроїв, захисту користувачів Інтернету від фішингу, вирішенням проблем використання паролів, а також розвиток доступності та безпеки біометричних технологій.

FIDO розробляє стандарти WebAuthn и CTAP, які будуть основою для різноманітних методів безпарольної автентифікації: біометричної, голосової, 2D-3D- фото, одноразових паролів та USB-ключів. На практиці користувачу буде запропоновано два типи ключів FIDO: ID-ключ – унікальний ідентифікатор, підключений до облікового запису в Інтернеті (аналог – соціальні мережі) та карта автентифікації. Для застосування карти автентифікації користувачу необхідно виконати певні процедури підтвердження його особи або використання апаратного ключа разом з біометричними або іншими унікальними даними, що підтверджують особу [14].

Стандарти FIDO генерує нову унікальну пару ключів на кожну нову і окрему транзакцію або реєстрацію, при цьому всі ключі зберігаються в безпечному сховищі типу SecureEnclave, TPM або TEE. Крім того, у FIDO потрібна тільки підтримка базової криптографії, ключі та біометрична інформація зберігається на безпечних чіпах і ніколи з них не вилучається [15].

Як бачимо, сьогодні сучасні технології IoT досить стрімко розвиваються. Водночас законодавство запізнюється в реагуванні на розвиток суспільних відносин із використанням технологій та пристроїв IoT. Досі відсутні єдині підходи до юридичного оформлення нормативної бази і в цій галузі. Більше того, немає одностайної наукової думки щодо класифікації ідентифікаційних та персональних даних, їх деталізації та однозначності формулювання дефініцій.

На цю ситуацію також звертає увагу в своїх дослідженнях Всесвітній Банк та Комісія Організації Об'єднаних Націй з міжнародного торговельного права, Міжнародної торгової палати і Європейської економічної комісії (UNCITRAL).

UNCITRAL задекларовано, що сьогодні є проблема формування кардинально однозначних дефініцій у сфері ідентифікаційних даних з метою прийняття їх усіма країнами та подальшого коригування національних законодавств до єдиного нормативного поля. Це сприятиме забезпеченню юридичного визнання та надання юридичної сили електронній ідентифікації та надання довірчих послуг, заборону певних видів дискримінації у зв'язку з використанням електронних засобів для перевірки ідентифікаційних даних. Також вказується на необхідність прийняття відповідних законів, які дозволяють управління ідентифікаційними даними, вимагають забезпечення та застосування конкретних процедур з метою оформлення, доставки та зберігання документів або облікових записів тощо [16].

В Україні також здійснюються заходи в напрямі організації та розвитку процесів електронної ідентифікації, які спрямовані на виключно технічні способи ідентифікації. Так, статтею 15 Закону України «Про електронні довірчі послуги» визначені схеми електронної ідентифікації.

Схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них. Схема електронної ідентифікації визначається Кабінетом Міністрів України.

Низький, середній та високий рівні довіри до засобів електронної ідентифікації повинні відповідати таким критеріям:

– низький рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує обмежений ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї належать, включаючи технічні засоби контролю, призначенням яких є зниження ризику зловживання або спростування ідентичності;

– середній рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує суттєвий ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є істотне зниження ризику зловживання або спростування ідентичності;

– високий рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує найвищий ступінь довіри до заявлених ідентифікаційних даних особи і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї належать, включаючи технічні засоби контролю, призначенням яких є запобігання зловживанню повноваженнями або підміні особи [17].

Постановою Кабінету Міністрів України від 19 червня 2019 № 546 «Про затвердження Положення про інтегровану систему електронної ідентифікації» визначено, що інтегрована система електронної ідентифікації – це інформаційно-телекомунікаційна система, яка призначена для

технологічного забезпечення зручної, доступної та безпечної електронної ідентифікації та автентифікації користувачів системи, сумісності та інтеграції схем електронної ідентифікації, їх взаємодії з офіційними веб-сайтами (веб-порталами), інформаційними системами органів державної влади, органів місцевого самоврядування, юридичних осіб і фізичних осіб – підприємців, забезпечення захисту інформації та персональних даних з використанням єдиних вимог, форматів, протоколів та класифікаторів, а також задоволення інших потреб, визначених актами законодавства.

Метою системи є забезпечення відповідно до схем електронної ідентифікації доступу користувачів системи до електронних послуг, які надаються органами державної влади, органами місцевого самоврядування, юридичними особами і фізичними особами – підприємцями, та їх сервісів, функціонування електронного документообігу, провадження іншої діяльності із застосуванням електронної ідентифікації. Система є складовою частиною інформаційно-телекомунікаційної інфраструктури, що забезпечує електронну взаємодію суб'єктів взаємодії з користувачами системи та забезпечує: проведення регламентних процедур та електронної ідентифікації користувачів системи для отримання ними електронних послуг, доступу до сервісів; взаємодію та сумісність з інформаційно-телекомунікаційними системами, які реалізують схеми електронної ідентифікації, та інформаційно-телекомунікаційними системами; дотримання вимог законодавства щодо захисту інформації та персональних даних; розвиток системи у напрямі інтеграції до інформаційно-телекомунікаційних систем для транскордонної електронної ідентифікації; інтеграцію інформаційно-телекомунікаційних систем суб'єктів взаємодії до системи [18].

Відповідно до постанови Кабінету Міністрів України від 19 червня 2019 №546 та згідно з ЄААД.468244.209 Д7.01 «Загальний опис. Інтегрована система електронної ідентифікації» Міністерством цифрової трансформації України ведуться роботи щодо створення інтегрованої системи електронної ідентифікації. Нині ця система надає тільки послуги перевірки цифрового підпису та підписання файлів цифровим підписом користувача без додаткових заходів ідентифікації підписантів і виступає в ролі транскодера між різноманітними системами ідентифікації, що створює низку суттєвих ризиків та правових невизначеностей і не сприяє зростанню довіри до державних цифрових сервісів, інформаційних ресурсів та технологій.

Крім того, наказом Державного агентства з питань електронного урядування від 27.11.2018 № 86 встановлено вимоги до засобів електронної ідентифікації (далі – Вимоги), рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування. Вимоги встановлюють організаційні, методологічні, технічні та технологічні умови використання засобів електронної ідентифікації у сфері електронного урядування залежно від рівнів довіри до засобів електронної ідентифікації. Ці Вимоги обов'язкові для виконання надавачами електронних довірчих послуг, підприємствами, установами та організаціями незалежно від форм власності, діяльність яких пов'язана з розробленням, виробництвом, сертифікаційними випробуваннями, експертними дослідженнями та експлуатацією засобів електронної ідентифікації, що видаються фізичним, юридичним особам або представникам юридичних осіб та використовуються для автентифікації у сфері електронного урядування [19].

Фактично вказаними нормативно-правовими актами закладено основу для формування технічних регламентів та законодавства у сфері управління ідентифікаційними даними, в тому числі і пристроїв IoT. Однак вказані нормативно-правові акти мають більш декларативний характер, ніж прикладний. На нашу думку, схема побудови технологічного транскодеру між різноманітними системами ідентифікації в Україні створює низку суттєвих ризиків та правових невизначеностей, що не сприятиме зростанню довіри до державних цифрових сервісів, інформаційних ресурсів та технологій.

Варто зазначити, що національне законодавство безперервно модернізується та поповнюється новими нормативно-правовими актами та дефініціями. Це водночас призводить до термінологічного розбалансування в сфері інформаційних технологій [20].

Також турбує й те, що українська законодавча база не відображає реальний стан реагування держави на правопорушення із використанням ідентифікаційних та персональних даних, а вкрай мінімізовані заходи державно-правового примусу не стримують повною мірою вчинення протиправних дій.

Внаслідок цифровізації діюча правова система в Україні не уникне трансформації. Найбільше потребують змін положення про відповідальність за правопорушення такого виду у Кримінальному кодексі та Кодексі про адміністративні правопорушення України. Відтак вкрай важливо проаналізувати весь набір дефініцій та розробити їх більш сучасні варіації [21].

Суттєвим ускладненням для функціонування систем управління ідентифікаційними даними є відсутність єдиного класифікатора ідентифікаційних даних [22]. Існує думка, що вирішення цієї проблеми доцільно розпочати із формування національного класифікатора на основі докумен-

тів, перелік яких визначено Законом України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус». Однак при цьому окремо необхідно вирішити цілий комплекс технічних та юридичних питань, пов'язаних із застосуванням біометричних даних, які можливо використовувати як елементи ідентифікації особи [23].

Невизначеності також додає і низка різних схем ідентифікації суб'єктів за ідентифікаційними даними. Наразі в Україні функціонують такі схеми ідентифікації, як «QsignID» (ідентифікатор – засоби кваліфікованого електронного підпису чи печатки), «BankID» (ідентифікатор – електронна анкета з ідентифікаційними даними користувача Системи BankID Національного банку України), «MobileID» (ідентифікатор – ідентифікаційна телекомунікаційна картка, в якій зберігається особистий ключ кваліфікованого електронного підпису), «PasscardID» (ідентифікатор – безконтактний електронний носій, в якому зберігається особистий ключ кваліфікованого електронного підпису та ідентифікаційні дані власника) та «Дія/Мій ID» (проєкт, ідентифікатор – електронна анкета з ідентифікаційними даними власника облікового запису у Національній системі електронної ідентифікації «Дія»).

Розбудова Інтегрованої системи електронної ідентифікації за методом декодера або шлюзу між різноманітними інформаційними ресурсами та системами ідентифікаційних даних, на нашу думку, є морально застарілим, малоефективним проєктом, який містить багато ризиків, передусім юридичних. Вектор всеохоплюючої цифровізації країни є безумовно прогресивним та сучасним рухом у розбудові України. Досвід, отриманий у ході підготовки концепції Інтегрованої системи електронної ідентифікації, безперечно доцільно врахувати під час розробки та впровадження сучасних правових механізмів управління ідентифікаційними даними та в подальшому створенні об'єднаної системи управління ідентифікаційними даними.

Об'єднана система управління ідентифікаційними даними – це багаторівнева соціотехніча система, за допомогою якої значна кількість людей має можливість взаємодіяти з багатьма підсистемами та технічними пристроями. За допомогою сучасних технологічних рішень на основі штучного інтелекту, комплексу сучасних технічних стандартів, юридичних правил та норм, порядків і процедур перевірки ідентифікаційних даних, система забезпечує тотожність ідентифікаційних даних з фізичною або юридичною особою, пристроєм або цифровим об'єктом під час здійснення транзакцій, а також зберігання і захист ідентифікаційних даних. Найголовнішим елементом системи стане сучасна нормативно-правова база регулювання суспільних відносин у сфері управління ідентифікаційними даними, яка визначить насамперед порядок транскордонного управління ідентифікаційними даними, права та обов'язки суб'єктів та об'єктів (систем із використання засобів штучного інтелекту), види протиправних суспільно небезпечних діянь та юридичну відповідальність за їх скоєння, передбачить порядок страхування транзакцій, забезпечить виконання зобов'язань сторін та відшкодування завданої шкоди тощо.

Головною процедурою такої системи стане процедура ідентифікації суб'єкта, яка надасть надійну та достовірну інформацію про те, хто насправді в даний момент часу надає запит на взаємодію із системою і проходить процедуру ідентифікації, автенифікації та авторизації. Такі процедури ідентифікації особи здійснюватимуться із застосуванням програмних методів на основі штучного інтелекту без втручання людського фактора.

Висновки. З урахуванням викладеного можливо констатувати наступні висновки.

Пристрої та технології IoT стають невіддільними складниками, які забезпечують функціонування різних сфер життєдіяльності людства.

Застосування пристроїв та технологій IoT формує нову електронну екосистему, що кардинально змінює відношення людства до результатів науково-технічної революції, а також ставлення особистості до процесів пізнання та сприйняття цифрової реальності, можливостей відтворення «віртуальної людини» за допомогою пристрів IoT та штучного інтелекту.

Темпи цифровізації суспільних відносин спонукають нормотворців та правознавців до активної модернізації законодавства, яке в сфері управління ідентифікаційними даними є архаїчним та малорозвинутим.

Інтеграція України в світові цифрові ринки та транскордонні електронні відносини повинна відбуватись одночасно із трансформацією національного законодавства із врахуванням передового світового досвіду в галузі управління ідентифікаційними даними.

Література

1. Протоколы передачи данных IoT. URL: https://iot.ru/wiki/protokoly-peredachi-dannykh-iot. (дата звернення: 19.05.2020).

2. Интернет вещей: LoRa устройства от Mikrotik. Lanmarket. 2019. URL: https://lanmarket.ua/stats/internet-veshchey-lora-ustroystva-ot-mikrotik (дата звернення: 29.08.2020).

3. Что такое IoT, или интернет вещей. URL: https://coinspot.io/beginners/chto-takoe-iot-ili-internet-veshhej. (дата звернення: 19.09.2020).

4. Internet of ThingsEU-China Joint White Paper on Internet-of-Things Identification EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS. European Communities, 2015. Reproduction authorised for non-commercial purposes provided the source

is acknowledge. 2015. URL: http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_EU-China_IoT_Identification_Final.pdf. (дата звернення: 10.10.2020).

5. Object Identifier (OID) Repository oid-info. 2020. URL: http://www.oid-info.com (дата звернення: 19.12.2020).

6. EPC та радіочастотна ідентифікація (РЧІ) «ДжіЕс1 Україна» URL: https://gs1ua.org/ua/gs1-system/epc. (дата звернення: 19.12.2020).

7. UUID (Universally Unique Identifier) Вікіпедія (wikipedia.org). 2018. URL: https://uk.wikipedia.org/wiki/UUID. (дата звернення: 09.01.2021).

8. Standard-based IoT platforms interworking: implementation, experiences, and lessons learned / Jaeho Kim, Sung-Chan Choi, Jaeseok Yun та ін.]. IEEE Communications Magazine. 2016. № 54. С. 48–54.

9. GS1 General SpecificationsThe foundational GS1 standard that defines how identification keys, data attributes and barcodes must be used in business applications. GS1 AISBL. 2020. URL: https://www.gs1.org/sites/default/files/docs/barcodes/GS1_General_Specifications.pdf. (дата звернення: 10.01.2021).

10. OCF Developer Program Open Connectivity Foundation. 2020. URL: https://openconnectivity.org/foundation/organizational-structure. (дата звернення: 19.03.2020).

11. Internet of things: Vision, applications and research challenges / D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac. Ad Hoc Networks. 2012. № 10. С. 1497–1516.

12. Андрощук Г. Інтелектуальна власність в системі інтернету речей: економіко-правовий аспект. *Теорія і практика інтелектуальної власності*. 2018. № 1. С. 65–73.

13. AIOTI Recommendations for future collaborative work in the context of the Internet of Things Focus Area in Horizon 2020 European Commission. 2020. URL: https://ec.europa.eu/digital-single-market/en/news/aioti-recommendations-future-collaborative-work-context-internet-things-focus-area-horizon-2020. (дата звернення: 15.12.2020).

14. Ходаковский К. Приступил к работе альянс FIDO, внедряющий новый стандарт аутентификации 3DNews Daily Digital Digest. 2013. URL: https://3dnews.ru/641590. (дата звернення: 29.12.2020).

15. Аккерманн Ю. Один из фундаментальных принципов FIDO Alliance – обеспечение приватности. *Хабр, Блог компании 1cloud.ru*. 2018. URL: https://habr.com/ru/company/1cloud/blog/416481/ (дата звернення: 28.12.2020).

16. Проект положений об использовании итрансграничном признании управления идентификационными данными и удостоверительных услуг. Представление Всемирного банка. Комиссия Организации Объединенных Наций по праву международной торговки. Рабочая группа IV (Электронная торговля). 2020. URL: https://undocs.org/ru/A/CN.9/WG.IV/WP.163. (дата звернення: 19.07.2020).

17. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення 16.08.2020).

18. Про затвердження Положення про інтегровану систему електронної ідентифікації: Постанова Кабінету Міністрів України від 19.06.2019 № 546 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/546-2019-п (дата звернення: 29.10.2020).

19. Про встановлення Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування: Наказ Державного агентства з питань електронного урядування від 27.1.2018 року № 86. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/RE32914.html (дата звернення: 29.10.2020).

20. Селезньова О.М. Нормативні дефініції в інформативному праві. *Правова інформатика.* 2014. № 1(41). С. 23–29.

21. Баулін Ю.В., Тацій В.Я. Завдання вітчизняної кримінально-правової науки в умовах реформування кримінального законодавства України. *Право України.* 2020. № 2. С. 17–31.

22. Баранов О.А. Основи класифікації інформаційного законодавства. *Правова інформатика.* 2006. С. 25–32. URL: http://ippi.org.ua/sites/default/files/06bokiz.pdf (дата звернення 01.12.2020).

23. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 р. № 5492-VI. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text.