КУЗЬМІН Д. В.,
кандидат юридичних наук,
викладач
*(Класичний фаховий коледж
Сумського державного університету)*

ЛЕМІШ Н. О.,
кандидат історичних наук, доцент,
викладач
*(Класичний фаховий коледж
Сумського державного університету)*

УДК 35.078.3
DOI https://doi.org/10.32842/2078-3736/2023.3.30

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ БЕЗПЕКИ ПЕРЕДАЧІ ІНФОРМАЦІЙНИХ ДАНИХ ПРО ФІЗИЧНИХ ОСІБ В УМОВАХ СТАНОВЛЕННЯ ТЕХНОЛОГІЙ ІНДУСТРІЇ 4.0

У статті проаналізовано основні загрози безпеки створення, передачі та збереження інформаційних даних про фізичних осіб в умовах становлення технологій Індустрії 4.0. Досліджена проблема створення та накопичення великого об'єму інформаційних даних у сучасних цифрових мережах. Визначено низку загроз, які безпосередньо впливають на ефективність забезпечення інформаційної безпеки в умовах становлення сучасних технологій Індустрії 4.0. Розглянуто проблеми, які впливають на ефективність правового регулювання безпеки передачі інформації про фізичних осіб в умовах розвитку сучасного онлайн середовища. Висвітлено проблему необхідності правового захисту інформації, що містить дані про особисті нематеріальні блага фізичних осіб в умовах розвитку технологій Індустрії 4.0, що тісно пов'язані з питаннями технологічних викликів. Зазначено, що під час обговорення питань інформаційної безпеки для фізичних осіб найсерйознішу проблему складає несанкціонований доступ з боку сторонніх суб'єктів до інформації, яка використовується державними органами та органами місцевого самоврядування. Відзначено, що ключовими генераторами великих об'ємів інформаційних даних залишаються державні органи, які створюють електронні сервіси з метою оптимізації системи управління та покращення якості надання громадянам адміністративних послуг. Відповідно створення технологічно передових продуктів, направлених на покращення ефективності державного управління, поліпшення якості сервісних послуг та підвищення швидкості обробки інформації з боку державних органів для її громадян, є вагомою перевагою. Проте збільшення кількості та функціоналу державних електронно-інформаційних сервісів, що передбачають ідентифікацію користувача, збір персональних даних, створення інформаційних баз, підвищує рівень загрози для безпеки збереження персональних даних фізичних осіб. Створення, поширення, збереження, доступ та відтворення інформації може (в інтересах держав, організацій, фізичних осіб) мати як негативні, так і позитивні наслідки. Тобто інформація та можливість її поширення є стратегічною складовою забезпечення безпеки.

Ключові слова: *інформація, інформаційні дані, четверта промислова революція, інформаційні дані про фізичних осіб, Індустрія 4.0.*

Kuzmin D. V., Lemish N. O. The issues of legal regulation of security of transmission of information about individuals under the conditions of formation of technologies of Industry 4.0

The article analyzes the main threats to the security of creation, transmission and storage of information data about individuals in the conditions of formation of technologies of Industry 4.0. The issue of creation and accumulation of a large amount of information data in modern digital networks has been studied. The article identifies a number of threats which have a direct impact on the effectiveness of information security in the context of the establishment of modern technologies of Industry 4.0. The article considers the challenges which influence the effectiveness of legal regulation of the security of the transmission of information about individuals in the conditions of development of the modern online environment. The problem of the need for legal protection of information, containing data on personal intangible goods of individuals under the conditions of development of technologies of Industry 4.0, closely connected with the issues of technological challenges, has been highlighted. The article notes that unauthorized access to information used by state and local self-government bodies is a serious problem when discussing information security for individuals. Government bodies which create electronic services to optimize the management system and improve the quality of providing administrative services to citizens have been pointed out to remain the key generators of large volumes of information. Accordingly, the creation of technologically advanced products aimed at improving the efficiency of public administration, improving the quality of services and increasing the speed of information processing by public authorities for its citizens, is a solid advantage. However, the increase in the number and functionality of state electronic information services which provide user identification, collection of personal data, creation of information databases, raise the threat to the security of the preservation of personal data of individuals. The creation, dissemination, storage, access and reproduction of information can have both negative and positive effects (for the benefit of the state, organizations, individuals). Thus, information and the possibility of its dissemination are a strategic component of security.

Key words: *information, information data, the fourth industrial revolution, information on individuals, Industry 4.0.*

Вступ. Протягом другої половини XX – початку XXI ст. відбулися визначні зміни в процесах, пов'язаних із передачею, збереженням та відтворенням інформації, які стали можливими в результаті розвитку науково-технічного прогресу, значно спростивши роботу людей із інформацією. Стрімке зростання використання інноваційних програм та продуктів, таких як сучасні цифрові інформаційні системи та мережі, хмарні обчислення, штучний інтелект призвели до появи нових комунікативних можливостей та стали причиною нових викликів, пов'язаних з питаннями безпеки. У результаті чого на рівні соціальних відносин, бізнесу та державного управління виникають проблеми з необхідністю адаптації системи управління та вдосконалення правових норм до потреб сучасності.

Під час розробки адаптивної стратегії реформування законодавства та системи управляння потрібно враховувати, що особливістю сучасного швидкозмінюваного онлайн середовища є досягнення у галузі роботи з цифровою інформацією. На концептуальному рівні ключові ідеї розвитку методів роботи з інформацією в умовах сучасного цифрового суспільства були висвітлені у праці Клауса Шваба, який обґрунтував теоретичні підходи до початку четвертої промислової революції, що реалізується шляхом поширення мобільного Інтернету, мініатюрності електронних пристроїв, розвитку штучного інтелекту [1, с. 7] та появою нових теоретичних обґрунтувань про поступовий перехід людства на технології Індустрії 4.0 [2]. Розвиток технологій у сфері комунікацій дозволили людству перейти на

новий технологічний щабель, що привело до появи нової проблеми, яка прямо пов'язана із розвитком сучасного інформаційно-цифрового простору, а саме: ключовою проблемою є актуальне питання наявності великого об'єму інформаційних даних (Big data) [3]. На думку деяких науковців, характерним явищем в часи «великих даних є процес безперервної їх генерації щомиті, таким чином, створюється їх велика різноманітність, що стає причиною неймовірно складної структури даних (неструктуровані/напівструктуровані) з питанням їх ідентифікації, сортування, пошуку, аналізу та візуалізації, що створює на сьогодні проблеми в стабільному функціонуванні організацій та безпечному житті фізичних осіб» [4].

Зазначимо, що під час організації роботи, пов'язаної з обробкою значних масивів інформаційних даних, виникають питання, у перу чергу, безпекового характеру для фізичних осіб. Збільшення кількості електронних пристроїв прийому-передачі цифрової інформації впливає на зростання активності та чисельності користувачів сучасного інтернет-середовища. Наслідком діяльності цього є процеси постійного росту об'єму інформаційних даних (Big data), що містять інформацію про персональні дані людей, їх професійну кар'єру, приватне життя та питання, пов'язані із правом власності, що призводить до збільшення числа загроз, обумовлює потребу у відповідному вдосконаленні національного законодавства України у сфері інформаційної безпеки.

Ураховуючи вищезазначене, вважаємо, що дослідження питань правового регулювання створення та передачі великого масиву інформаційних даних (Big data), які стосуються фізичних осіб, є актуальним та складає одне із ключових проблем безпеки, відповідно до сучасного технологічного рівня розвитку людства.

Проблемам створення та поширення великого масиву інформаційних даних присвятили дослідження чимало вітчизняних науковців, а саме: О.А. Баранов, В.М. Брижко, М.В. Гуцалюк, Р.А. Калюжний, О.М. Капля, Б.А. Кормич, В.А. Ліпкан, А.Л. Правдюк, А.І. Марущак, В.С. Цимбалюк, М.Я. Швець тощо. Проте проблеми правового регулювання забезпечення інформаційної безпеки даних про фізичних осіб в умовах постійно зростаючого великого об'єму інформаційних даних залишаються малодослідженими.

Постановка завдання. Мета статті полягає в аналізі та висвітленні ключових проблем, пов'язаних з правовим регулюванням створення, передачі та поширення великого об'єму інформаційних даних (Big data) про фізичних осіб та забезпечення їх безпеки в контексті розвитку технологій Індустрії 4.0.

Результати дослідження. Для проведення подальшого дослідження визначимося з ключовим тлумаченням терміну «інформація». Автори «Юридичної енциклопедії» термін «інформація» трактують як «документальні або публічно оголошені відомості про події та явища, що відбуваються у суспільстві й державі та навколишньому природному середовищі» [5, с. 717]. Законодавче визначення терміну «інформація» міститься в Статті 1 Закону України «Про інформацію» [6] та статті 200 Цивільного кодексу України [7]. Відповідно до зазначеного Закону: «інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [6].

Відомий вітчизняний дослідник інформаційного права О. Баранов, проаналізувавши наявні в українському законодавстві підходи до визначення терміну «інформація» та окресливши їх логічні недоліки, запропонував своє визначення вищезгаданого терміна, де під «інформацією розуміються відомості, представлені в будь-якій організаційній формі та вигляді, на будь-яких носіях, про події і явища, які мали або мають місце в суспільстві, державі і навколишньому середовищі» [8, с. 116-117].

Поширення інформації в соціумі має унікальну властивість впливу на свідомість та може виступати причиною мотивації соціальної поведінки, як окремих громадян так і об'єднаних ними соціальних груп. Створення, поширення, збереження, доступ та відтворення інформації може (в інтересах держав, організацій, фізичних осіб) мати як негативні, так і позитивні наслідки. Тобто інформація та можливість її поширення є стратегічною складовою забезпечення безпеки. Інформація та методи її поширення, маючи соціальну значущість, потребують правового регулювання, у тому числі й тих аспектів, які пов'язані із забезпечен-

ням безпеки поширення інформаційних даних про фізичних осіб. Зазначена позиція знайшла своє відображення в Законі України «Про інформацію», де окреслені принципові положення щодо забезпечення інформаційної безпеки з боку держави. Згідно зі Статтею 2 Закону передбачено правомірність одержання, використання, поширення, зберігання та захисту інформації. Встановлений принцип захисту особи від втручання в її особисте та сімейне життя [6].

Винайдення нових методів комунікації та передачі великих об'ємів даних в умовах становлення Індустрії 4.0 підсилює небезпеку від вже раніше виявлених загроз та формує джерельну базу до виникнення нових, ще не визначених загроз. Ураховуючи вищезазначене, вважаємо за доцільне проаналізувати можливі загрози, пов'язані з інформаційною безпекою для громадян. Розуміючи, що інформаційні атаки на дані, пов'язані з ідентифікацією людей, їхнім життям та діяльністю, переслідують низку цілей, які можуть бути як взаємопов'язані між собою, так і мати одноразові несистемні дії. Найчастіше метою інформаційної атаки є дії, направлені на: розголошення приватної інформації про фізичних осіб; дискредитацію окремих громадян та завдання репутаційних збитків організаційним структурам, що співпрацюють з громадянами; одержання нелегального доходу від використання інформаційних даних про громадян.

Становлення Індустрії 4.0 ґрунтується на широкому використанні інформаційних ресурсів, їх функціонал критично пов'язаний з необхідністю ідентифікації, збирання та накопичення даних про фізичних осіб та їх використання для здійснення сервісного обслуговування громадян. Зазначене обумовило характерну особливість сьогодення – створювати бази даних для забезпечення ефективної діяльності окремими громадянами, суб'єктами підприємницької діяльності та органами державного управління. Постійна тенденція до зростання кількості даних та технічної інфраструктури, де вони зберігаються, зумовлює збільшення числа даних про фізичних осіб та підвищує варіативність інформаційних загроз безпеки фізичних осіб та захисту їх особистих нематеріальних благ. Правовий захист особистих нематеріальних благ фізичних осіб включає, згідно Цивільного кодексу України, два наступні аспекти: захист приватності та захист прав інтелектуальної власності. Так, законодавець у статті 201 Цивільного кодексу України до переліку особистих немайнових благ, що потребують забезпечення безпеки, відніс: здоров'я, життя; честь, гідність і ділова репутація; ім'я (найменування); авторство; свобода літературної, художньої, наукової і технічної творчості, а також інші блага, які охороняються цивільним законодавством [7]. Проблема правового захисту інформації, яка містить дані про особисті нематеріальні блага фізичних осіб в умовах розвитку технологій Індустрії 4.0 тісно пов'язана з питаннями технологічних викликів, де реалізація традиційних методів правового захисту громадян з боку держави може бути не ефективною.

Унаслідок реалізації завдань зі створення та цілеспрямованого збирання різними програмними продуктами цифрових інформаційних даних про людину протягом всього її життя, накопичується значний архів неструктурованих, необ'єднаних до єдиної системи архів інформаційно-цифрових даних, які мають різний рівень забезпечення безпеки та надання можливого доступу до них з боку суб'єктів господарювання та державних органів, які їх адмініструють. Ці дані мають різну форму, представлені різними базами, реєстрами, кадастрами, пропозиціями сервісних, торгівельних та розважальних платформ тощо. Інформаційні дані про себе та свою діяльність фізичні особи переважно залишають подібним онлайн сервісам у добровільному порядку, бажаючи отримати певний доступ до цифрових ресурсів та сервісів. Такі потреби людей пов'язанні з необхідністю сервісного обслуговування, адміністрування під час організації дозвілля, підприємницької та управлінської діяльності, постійно збільшують об'єм великих даних, сформувавши таке явище, яке отримало назву цифровізація. Вона вплинула на процеси пов'язані із легкою доступністю людей до інформації на глобальному економічному рівні, створивши сучасну модель глобальної економіки. Зазначене дозволило дослідникам І.С. Ткаченко та В.В. Шарко відзначити, що «за досягнення найбільш складних рівнів цифровізації в економіці відбувається кардинальна трансформація виробничих відносин учасників, результатом якої є об'єднання виробництва й послуг в єдину цифрову (кіберфізичну) систему». [9, с. 44].

Більше того, саме сучасна прогресивна економічна концепція Інтернету речей (Internet of Things) [10] побудована на ідеях всепоглинаючої автоматизованої інформаційної системи, що об'єднує та дозволяє взаємодіяти між собою людям та різним речам сучасної матеріальної культури, об'єднаних між собою єдиною мережею. Так ідеї, як розумні речі, розумний дім, розумне робоче місце, розумний транспорт – усе це є складовими вищеозначеної системи. Фізичні особи, які все більше звертаються до розумної електроніки, змушені погоджуватися в добровільному порядку на передачу даних про свою діяльність, що з кожним роком (у зв'язку з збільшенням чисельності розумної електроніки та людей, які бажають або змушені її використовувати) постійно зростає. Дослідники з безпеки великих даних Е. Бертіно та Є. Феррарі відзначають, що «до наявних проблем інформаційної безпеки додаються нові, причиною яких є поява все нових способів збирання та обробки даних, які використовуються в системі Інтернет речей, що веде до зростання потенціалу атак» [11].

Нині навіть важко уявити рівень каталогізації та об'єм всього масиву інформаційних даних про діяльність фізичних осіб, які зберігаються, та до яких можливо отримати доступ за допомогою мережі «Інтернет», що постійно збільшує загрозу та функціонал атак, пов'язаних із несанкціонованим доступом до інформації. Так, відомий науковець О. Баранов, коментуючи вищезазначені проблеми, відзначив що «інтернет речей базується на масштабному використанні датчиків, що генерують потоки даних, обчислювальних ресурсів і комп'ютерних програм, мережі Інтернет, що веде до правових проблем» [12, с. 101].

Враховуючи вищезазначене, вважаємо, що одним із складових завдань, метою яких є забезпечення безпеки фізичних осіб, виступає захист персональних даних про людину та даних про її життя у всезростаючому масиві інформації. На законодавчому рівні Статтею 11 Закону України «Про інформацію» зазначено, що «інформацією про фізичну особу (персональні дані) визначає відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [6]. Цифрова ідентифікація фізичної особи в сучасному онлайн-середовищі відіграє важливу роль. Завдяки їй є можливість забезпечити певні заходи безпеки, захистивши користувачів від шахрайських дій, крадіжки особистих даних, недопущення несанкціонованого доступу до цифрових ресурсів. Що, відповідно, дозволяє фізичним особам користуватися різноманітними онлайн-послугами, такими як банківське обслуговування та інтернет-торгівля, цифрові комунікативні системи, мережеві технології та автоматизація, отримання послуг від державних органів на основі електронного адміністрування.

Проте, відзначимо, що темпи, які набрала цифровізація, постійно зростають, збільшуючи об'єм інформації, пов'язаної із персональними даними, збільшується число програмних продуктів, функціонал яких побудований на процесі ідентифікації людини. Цей процес стає причиною збільшення чисельності загроз інформаційного характеру для фізичних осіб. Тобто число загроз несанкціонованого доступу до особистої інформації фізичних осіб зростає, арсенал методів та інструментів для реалізації атак на дані у великому масиві розширюється, їх проводити стає легше. Крім того, наявність проблем великого об'єму даних збільшує можливість помилки адміністратора та складність ідентифікації безпосередньої атаки. Як зазначають дослідники з безпеки великих даних, «серйозною загрозою є підробка даних та проблеми, пов'язані з даними, які містять помилки» [13, с. 276].

Сьогодні проблема захисту персональних даних вийшла далеко за межі українського національного законодавства, ставши глобальною світовою проблемою. Великі об'єми інформаційних персональних даних не мають фізичних обмежень при перетинанні кордону. Самі інформаційні дані можуть бути використані в інших країнах із метою нанесення матеріальної та репутаційної шкоди завдяки розвитку швидкісного Інтернету, що зумовлює, на думку О.А. Баранова та В.М. Брижко «цілеспрямовану необхідність здійснювати правовий вплив на регулювання транскордонних потоків персональних даних» [14, с. 90].

Таким чином, розвиток сучасних технологій Індустрії 4.0 доповнив перелік загроз, складовими яких є інформаційні дані про діяльність людей, таємницю листування, пересування, місця перебування, фінансового стану та стану здоров'я. Відзначимо, що до масового

поширення сучасних мережевих технологій, зібрана інформація, яка надавала можливість ідентифікувати фізичну особу, не несла серйозні моральні та матеріальні загрози для громадян. Але на сучасному рівні розвитку цифрових технологій поширення навіть елементарних даних про фізичних осіб стає джерелом небезпеки. Держава, яка взяла на себе обов'язок із забезпечення безпеки її громадян, змушена реагувати на сучасні інформаційні виклики, встановлюючи пріоритети розвитку вітчизняного законодавства. Так, ключові пріоритети, пов'язані із забезпеченням безпеки для громадян, визначені в Статті 3 Конституції України, де людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю [15]. Саме для забезпечення інформаційної безпеки органи державної влади здійснюють цілеспрямований вплив на свідомість громадян з метою зменшення загроз та ризиків від інформаційно-цифрових загроз шляхом впровадження законодавчих норм. Як приклад законодавчого впливу на інформаційне-цифрове середовище, приведемо Статтю 6 Закону України «Про інформацію», де визначено, що право на інформацію може бути обмежене «для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно» [6].

Відзначимо, що забезпечення інформаційної безпеки є, у першу чергу, завданням держави, що встановлено Статтею 17 Конституції України та «Стратегією інформаційної безпеки», затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021 [16]. Діяльність держави спрямована на організацію та управління соціальними процесами, що відбуваються на її території. Зрозуміло, що в межах управління держава змушена протистояти загрозам безпеки як внутрішнім, так і зовнішнім. З метою реалізації саме таких функціональних завдань держава створює інформаційні системи протидії загрозам інформаційної безпеки, серед яких можливо виокремити технічні, комунікаційні, адміністративні та правові компоненти.

У «Стратегії інформаційної безпеки» міститься перелік загроз інформаційної безпеки, серед яких назвемо наступні: «глобальні дезінформаційні кампанії, спеціальні інформаційні операції вороже налаштованих держав, соціальні мережі як суб'єкти впливу в інформаційному просторі, низький рівень медіаграмотності, несформованість системи стратегічних комунікацій, спроби маніпуляції свідомістю громадян» [16].

«Стратегія інформаційної безпеки» означила завдання із запобігання та протидії загрозам інформаційної безпеки. Серед яких стратегічно правильним є постановка завдання із «створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам та максимально швидке виявлення та реагування держави й суспільства на інформаційні загрози» [16]. Але реалізація завдань із забезпечення інформаційної безпеки, згідно програмним завданням Стратегії, має низку проблемних моментів. Визначимо деякі питання цієї проблематики: технічна складова структури сучасного інтернет-простору базується якраз на децентралізованих (хоч і об'єднаних в єдину мережу) серверах, географічно розташованих на різних територіях, не обмежений транскордонний рух інформації, де, як зазначає І.Р. Боднар, кожна держава є частиною світового інформаційного простору [17, с. 70], блокувати яку інколи окремо взятій державі буває на програмному рівні проблематично. Сам великий об'єм інформаційних даних (Big data) важко швидко проаналізувати та виявити проблеми, які потребують оперативного втручання з боку суб'єкта адміністрування.

Також з боку громадян є суспільний запит, про наявність якого згадує група вітчизняних дослідників, де «державна інформаційна політика має забезпечувати свободу інформації, сприяти розвитку нових інформаційно-комунікаційних технологій, створювати більш відкрите управління суспільними програмами» [18]. Названі позиції з боку держави встановлені у Статті 2 Закону України «Про інформацію», де надаються гарантії громадянам на відкритість, доступність інформації, на свободу обміну інформацією [6]. Таким чином, сучасна держава змушена здійснювати власну регуляторну політику щодо забезпечення інформаційної безпеки, дотримуючись позицій певного балансу між свободою поширення даних та обмежень, ціль яких полягає в захисті збереження великих об'ємів інформації про фізичних осіб з урахуванням розвитку сучасних інформаційно-електронних технологій.

Під час обговорення проблем інформаційної безпеки для фізичних осіб зазначимо, що найсерйознішу проблему складають якраз несанкціонований доступ з боку сторонніх суб'єктів до інформації, яка використовується державними органами та органами місцевого самоврядування. Державні органи, створюючи електронні сервіси, метою яких є оптимізація системи управління та покращення якості надання громадянам адміністративних послуг, залишаються ключовими генераторами великих об'ємів інформаційних даних про фізичних осіб. Створення технологічно передових продуктів, направлених спрямованих на покращення ефективності державного управління, поліпшення якості сервісних послуг та підвищення швидкості обробки інформації з боку державних органів для її громадян, є вагомою перевагою. Проте, збільшення кількості та функціоналу державних електронно-інформаційних сервісів, що передбачають ідентифікацію користувача, збір персональних даних, створення інформаційних баз, підвищує рівень загрози для безпеки збереження персональних даних, що стосуються фізичних осіб.

На сьогодні серед науковців побутують різні підходи щодо нарямів забезпечення безпеки інформації. Одним із методів забезпечення інформаційної безпеки з боку держави є підхід, запропонований вітчизняними науковцями, щодо необхідності органів влади діяти на основі єдиних правил та стандартів від національного до регіональних [19, с. 100]. Іншим напрямом забезпечення безпеки є адміністративний метод примусу. Держава на рівні нормативно-правового регулювання може обмежити доступ до інформації згідно Статті 6 Закону України «Про інформацію» [6]. Деякі держави в цьому напрямі застосовують доволі жорсткий режим персональної ідентифікації користувача, який приєднується до інтернету. При обранні державними органами подібних стратегій відбуваються, як відмічає О.М. Капля, процеси, де «інформаційна безпека громадянина значною мірою трансформується, вона спрямована більше не на захищеність окремих його прав, як особистості, а на загальний захист інтересів суспільства» [20. с. 19].

Ще одним напрямом захисту даних про фізичних осіб з боку суб'єктів господарської діяльності, є напрям, пов'язаний з інформаційно-електронними процедурами, сервісами та послугами, без яких взагалі цілій низці галузей економіки не можливо вести свою господарську діяльність. Робота з електронно-інформаційними програмами та каталогами є складовою праці найманих працівників, що й сприяє зростанню об'єму персональних даних про фізичну особу, пов'язану з діяльністю суб'єктів господарювання. Цей напрям потребує особливої уваги, яка буде направлена на забезпечення інформаційної безпеки, адже кількість цифрових інформаційних даних про фізичних осіб значна, проте рівень забезпечення безпеки переважно комерційних структур, порівняно із державними органами, може знаходитись у гіршому стані. Зазначене вказує на нагальну потребу удосконалення вітчизняного законодавства із забезпечення інформаційної безпеки при взаємодії господарюючих суб'єктів (при цифровій реєстрації та збереженні даних про громадян) та фізичних осіб.

Отже, розвиток технологій Індустрії 4.0 відкриває нові можливості для здійснення соціальних комунікацій, розвитку бізнесу та удосконалення системи адміністративного управління державою. Проте виникають нові загрози, які пов'язані із захистом інформації про фізичних осіб, що негативно впливає на безпеку передачі даних. З метою забезпечення інформаційної безпеки слід вжити заходи з активізації міжнародного співробітництва, розробляти єдині стандарти та протоколи доступу до персональних даних фізичних осіб.

Висновки. Розвиток цифрових технологій, що використовуються в Індустрії 4.0, призводить до збільшення обсягу та складності передачі інформаційних даних про фізичних осіб. Нині забезпечення безпеки під час поширення значних об'ємів інформаційних даних (Big data) про фізичних осіб формує два основні напрями правового регулювання з боку держави, визначимо їх як: захист даних про фізичних осіб з боку суб'єктів господарської діяльності та захист даних про фізичних осіб, пов'язаних з організацією функціонування державних структур. Ураховуючи всезростаюче значення забезпечення безпеки великого об'єму даних (Big data) про фізичних осіб, виникає потреба впровадження державними органами загальноприйнятних, інституційно та технічно можливих стандартів та протоко-

лів забезпечення інформаційної безпеки, що повинна базуватися на відповідності правових норм потребам сучасного технічного розвитку людства.

Список використаних джерел:

1. Schwab, K. The fourth industrial revolution. Currency. 2017.
2. Lasi, H., Fettke, P., Kemper, H. G., Feld, T., & Hoffmann, M. Industry 4.0. *Business & information systems engineering.* 2014. 6, С. 239-242. https://link.springer.com/article/10.1007/s12599-014-0334-4.
3. Shi, Yong. Advances in big data analytics: theory, algorithms and practices. *Springer Nature*, 2022.
4. Naeem, M., Jamal, T., Diaz-Martinez, J., Butt, S. A., Montesano, N., Tariq, M. I., De-La-Hoz-Franco E., De-La-Hoz-Valdiris, E. Trends and future perspective challenges in big data. In Advances in Intelligent Data Analysis and Applications. Springer, Singapore. 2022. pp. 309-325.
5. Юридична енциклопедія: в 6 т. / за ред. Ю.С. Шемчушенка. К.: Українська енциклопедія, 1998–2004. Т. 2. 1999. 744 с.
6. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
7. Цивільний кодекс України від 16.01.2003 р. № 435-IV / *Верховна Рада України*. URL: http://zakon2.rada.gov.ua/laws/show/435-15.
8. Баранов О. Інформаційне право України: стан, проблеми, перспективи. К. 2005. 369 с.
9. Ткаченко І.С. та Шарко В.В. Конкурентоспроможність підприємства в умовах цифрової економіки. *Вісник Хмельницького національного університету*. 2022. № 1. С. 43-48.
10. Li, S., Xu, L. D., & Zhao, S. (2015). The internet of things: a survey. *Information systems frontiers*, *17*, 243-259. https://link.springer.com/article/10.1007/s10796-014-9492-7.
11. Bertino, Elisa, and Elena Ferrari. "Big data security and privacy." A comprehensive guide through the Italian database research over the last 25 years. Springer, Cham, 2018. 425-439. https://link.springer.com/chapter/10.1007/978-3-319-61893-7_25.
12. Баранов О. «Інтернет речей» як правовий термін. *Юридична Україна*. 2016. № 5-6. С. 96-103.
13. Zhang, Dongpo. Big data security and privacy protection. In: 8th International Conference on Management and Computer Science (ICMCS 2018). Atlantis Press, 2018. p. 275-278. https://www.atlantis-press.com/proceedings/icmcs-18/25904185.
14. Баранов О. А., Брижко В. М., Захист персональних даних в сфері інтернет речей. *Інформація і право*. 2016. № 2 (17). С. 85-91.
15. Конституція України: Закон України від 28 червня 1996 року р. № 254к/96-ВР / *Верховна Рада України*. URL: http://zakon3.rada.gov.ua/laws/show/254к/96-вр.
16. Стратегія інформаційної безпеки затверджена Указом Президента України від 28 грудня 2021 року № 685/2021 / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.
17. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки.* 2014. № 1. С. 68-75.
18. Глушко А. Д., Панталь В. В., Бабенко С.. Інформаційна політика в системі забезпечення фінансової безпеки держави. *Ефективна економіка.* 2022. № 2. http://reposit.nupp.edu.ua/bitstream/PoltNTU/10415/1/Стаття_Глушко_Пантась_Бабенко.pdf.
19. Дурман О. Л., Хмельницька М.В., Методологічні аспекти розвитку цифровізації державних органів. *Вісник Херсонського національного технічного університету*. 2022. 1 (80). С. 94-102.
20. Капля О. М. Правове регулювання інформаційної безпеки громадянина під час дії воєнного стану. *Експерт: парадигми юридичних наук і державного управління*. 2022. 6 (24). С. 16-20.