УДК 342.9 (477)
DOI https://doi.org/10.32782/ln.2024.24.10

Бондар Д.В.
кандидат наук з державного управління,
ректор
Львівський державний університет безпеки життєдіяльності

ДОСВІД АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

Вступ. Україна прагне набути повноправного членства в Європейському Союзі, тому пріоритетним завданням національних органів публічної адміністрації є адаптація національного законодавства до права ЄС. Однією із основних сфер суспільних відносин, яка потребує належного адміністративно-правового регулювання у відповідності до європейських стандартів, є безпека життєдіяльності. Співробітництво у сфері цивільного захисту передбачено зокрема Угодою про асоціацію між Україною та Європейським Союзом.

Враховуючи вищезазначене, дослідження досвіду адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі має як теоретичне, так і практичне значення.

Питанням забезпечення безпеки життєдіяльності приділяють увагу науковці з різних галузей наукового знання. З останніх досліджень присвячених вказаній тематиці варто виділити роботи таких відомих науковців як Ф. Апшай, Т. Гринюк, К. Марченко, О. Оришака, О. Остапенко, О. Халак, О. Хитра, О. Чекригін та інші дослідники.

Правове регулювання використання інформаційних технологій (цифровізації) у різних сферах суспільного життя досліджували такі відомі науковці як М. Бабик, В. Бевзенко, Д. Біленька, О. Берназюк, М. Віхляєв, О. Гунбіна, К. Дубова, С. Єсімов, Т. Ковальова, Т. Коломоєць, О. Комаров, А. Комзюк, А. Краковська, І. Лопушинський, К. Оксютенко, А. Омельченко, М. Серебро, Р. Стефанчук, І. Тищенкова та інші.

Проте, досвід адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в країнах-членах Європейського Союзу ще не був предметом окремого наукового аналізу, що актуалізує необхідність підготовки даної публікації.

Постановка завдання. Метою публікації є дослідження досвіду адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в країнах-членах Європейського Союзу.

Методологія даної публікації традиційно об'єднує три групи методів наукового пошуку. Першу групу складають філософські методи дослідження, а саме, метод діалектики, його закони та прийоми, а також метод метафізики. Серед загальнонаукових методів дослідження (друга група методів) більшою мірою застосовуються прийоми логіки (аналіз, синтез, дедукція, індукція, порівняння), системний та структурно-функціональний методи. Третю групу складають спеціально-юридичні методи дослідження, серед яких більшою мірою застосовується методологія порівняльного правознавства, а також формально-юридичний метод та метод юридичного моделювання.

Виклад основного матеріалу. Починаючи дослідження європейського досвіду адміністративно-правового регулювання викори-

стання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід зазначити, що цифровізація публічного управління взагалі є одним із пріоритетних напрямів політики ЄС.

І. Белова, О. Ярощук та А. Гомотюк зазначають, що одним із важливих факторів високого рівня цифровізації сектору публічних послуг, суспільних та економічних процесів Європейського Союзу є інституціональний аспект, адже на рівні спільноти у 2015 році було затверджено стратегію Єдиного цифрового ринку, основними цілями якої стали: усунення регуляторних бар'єрів шляхом гармонізації правил та норм ЄС у різних секторах, включаючи електронну комерцію, авторське право, захист даних і телекомунікацій з метою полегшення транскордонної діяльності бізнесу; сприяння транскордонній електронній комерції шляхом створення рівних умов для електронної комерції в ЄС, дозволяючи споживачам і підприємствам купувати та продавати товари та послуги онлайн легше та з більшою впевненістю; підвищення інновацій шляхом підтримки стартапів, малих і середніх підприємств, полегшення доступу до фінансування та сприяння розвитку нових цифрових технологій і послуг; підвищення кібербезпеки. Функціонування єдиного цифрового ринку має на меті посилити кібербезпеку та захист даних у всьому ЄС, гарантуючи, що всі громадяни та підприємства ЄС можуть скористатися можливостями, які надають цифрові технології, одночасно захищаючи свою конфіденційність і безпеку [1, с. 182].

Отже, однією з основних цілей функціонування єдиного цифрового ринку ЄС є посилення кібербезпеки та захист даних на території всього Європейського Союзу, що фактично є частиною системи забезпечення безпеки життєдіяльності громадян держав-членів ЄС.

Одним із аспектів Стратегії єдиного цифрового ринку став План дій електронного уряду на 2016-2020 роки, в якому викладено бачення ЄС єдиного цифрового ринку та окреслено конкретні дії, які необхідно вжити для покращення послуг електронного урядування в ЄС. Він зосереджений на покращенні доступності, орієнтованості на користувача та сумісності державних послуг.

Окрім цього, у жовтні 2017 року в ЄС було прийнято Таллінську декларацію про електронний уряд, де було викладено бачення розвитку цифрових публічних послуг у ЄС та окреслено ключові принципи і пріоритети для досягнення цього бачення, серед яких одне з ключових місць посідає забезпечення безпеки та конфіденційності цифрових державних послуг і зміцнення довіри громадян за допомогою відкритих стандартів і сумісних систем. Також в декларації зазначено, що уряди повинні сприяти інноваціям та експериментам у розробці цифрових державних послуг, використовуючи новітні технології, такі як штучний інтелект і блокчейн, для підвищення ефективності та результативності [1, с. 182–183].

Таким чином, Таллінська декларація стала основою для формування національних законодавств держав-членів ЄС у сфері цифровізації публічних послуг та електронного урядування.

І. Белова, О. Ярощук та А. Гомотюк також зазначають, що окрім Таллінської декларації про електронний уряд, важливими документами щодо регулювання розвитку цифровізації в Європейському Союзі є: Європейська структура сумісності (EIF), яка надає загальний набір стандартів і вказівок для забезпечення легкого доступу до державних послуг і спільного використання в усьому ЄС; Регламент eIDAS, що визначає правила електронної ідентифікації та довірчих послуг у всьому ЄС; Загальний регламент захисту даних (GDPR), який встановлює правила обробки персональних даних у ЄС. Таким чином, Європейський Союз за короткий проміжок часу сформував нормативно-правове поле процесів цифровізації публічних послуг [1, с. 182–183].

У березні 2021 року Європейська Комісія запропонувала шлях до Цифрового десятиліття. Ця політична програма керується

«Цифровим компасом до 2030 року» – планом досягнення цифрової трансформації економіки та суспільства ЄС. Зазначений цифровий компас спрямований на безпечну цифрову екосистему, орієнтовану на людину, де громадяни отримують повноваження, а компанії процвітають завдяки цифровому потенціалу. Компас вказує чотири кардинальні точки для цієї траєкторії: цифрові навички, безпечна та ефективна цифрова інфраструктура, цифрова трансформація бізнесу та цифровізація державних послуг [2].

Отже, одним із пріоритетів цифрової стратегії ЄС є забезпечення безпечної цифрової інфраструктури, тобто фактично забезпечення безпеки життєдіяльності громадян ЄС в цифровому просторі та у суспільних відносинах, пов'язаних із використанням цифрових інструментів.

Вказаний політичний порядок денний узгоджується з нормами та стандартами ЄС для посилення цифрового суверенітету ЄС. Низка бюджетних інструментів підтримуватиме інвестиції, необхідні для побудови Цифрового десятиліття Європи на міцній основі. Оскільки цифрові технології є пріоритетом ЄС, вони також є пріоритетними для країн-стратегічних партнерів ЄС щодо створення кращого та більш гармонізованого цифрового середовища. Цілі політики Східного партнерства на період після 2020 року включають цільові дії, які сприятимуть розвитку Єдиного цифрового ринку: інвестиції в конкурентоспроможні та інноваційні економіки, у людей і розвиток знань, у безпеку та кіберстійкість, а також у цифрову трансформацію [2].

Таким чином, для національних органів публічної адміністрації в контексті євроінтеграційних процесів важливо приймати активну участь у розвитку Єдиного цифрового ринку ЄС, залучати інвестиції для розвитку національного цифрового ринку, включаючи заходи із забезпечення кібербезпеки.

Так, Міністерство цифрової трансформації України відповідно до покладених на нього завдань:

– організовує та координує діяльність органів виконавчої влади, пов'язану з інтеграцією України до Єдиного цифрового ринку ЄС (EU Digital Single Market), а також участю України у програмах ЄС щодо цифрового співробітництва, зокрема у Програмі ЄС «Цифрова Європа» (Digital Europe Programme);

– розробляє акти з метою забезпечення виконання завдань, пов'язаних з участю України у Програмі ЄС «Цифрова Європа» (Digital Europe Programme), зокрема щодо процедури визначення кандидатур для включення у мережу Європейських цифрових інноваційних хабів (European Digital Innovation Hubs) [3].

Крім того, у відповідності до п. 7 Положення ро Міністерство цифрової трансформації України, затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856, Мінцифри у процесі виконання покладених на нього завдань взаємодіє в установленому порядку з іншими державними органами, допоміжними органами і службами, утвореними Президентом України, тимчасовими консультативними, дорадчими та іншими допоміжними органами, утвореними Кабінетом Міністрів України, органами місцевого самоврядування, об'єднаннями громадян, громадськими спілками, профспілками та організаціями роботодавців, відповідними органами іноземних держав і міжнародних організацій, а також з підприємствами, установами та організаціями [3].

Отже, в процесі адміністративно-правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності відповідному органу публічної адміністрації, який реалізує державну політику у сфері цивільного захисту, доцільно взаємодіяти із Міністерством цифрової трансформації України та здійснювати правове врегулювання вказаних питань за допомогою спільних наказів.

Окрему увагу в контексті правової регламентації використання інформаційних технологій у сфері забезпечення безпеки жит-

тєдіяльності в Європейському Союзі слід приділити GDPR – Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних; про відміну Директиви 95/46/ЄС (GDPR набрав чинності 25 травня 2018 року) [4].

Основні вимоги GDPR: дотримуватися принципів обробки персональних даних; персональні дані слід обробляти прозоро, справедливо та законно (Lawfulness, fairness and transparency); персональні дані можна обробляти лише для явно вказаних законних цілей (Purpose limitation); збирати та зберігати слід лише мінімальну кількість персональних даних, достатніх для зазначеної мети (Data minimisation); персональні дані мають обмежений термін зберігання, не більше ніж це необхідно для певної мети (Storage limitation); забезпечення точності персональних даних, а також можливості їх редагування та видалення (Accuracy); забезпечення безпеки, цілісності та конфіденційності персональних даних (Integrity and confidentiality); контролер повинен бути готовим і здатним продемонструвати дотримання вищезазначених принципів (Accountability); реалізовувати права суб'єктів даних (право бути поінформованим, право на доступ, право на виправлення даних, право на видалення, право на обмеження обробки, право на мобільність даних, право на заперечення, право не бути об'єктом автоматизованого рішення, у тому числі профайлінгу, право на ознайомлення з Політикою приватності (Privacy Policy) та Політикою використання файлів cookie (Cookie Policy) [4].

Крім того, кожен суб'єкт даних має право на подання скарги до контролюючого органу, без обмеження будь-якого іншого адміністративного чи судового засобу правового захисту. Суб'єкт даних має право безпосередньо звернутися до суду для захисту своїх прав та інтересів. Відповідно до ст. 82 GDPR будь-яка особа, яка зазнала матеріальної чи моральної шкоди внаслідок порушення Регламенту, має право на отримання відшкодування від контролера або процесора за заподіяну шкоду [4].

За порушення вимог GDPR передбачені наступні адміністративні штрафи: до 10 млн. євро або 2% від світового річного обороту (залежно що більше) за незначні порушення; до 20 млн. євро або 4% від світового річного обороту (залежно що більше) за серйозні порушення, до яких належать порушення контролером та процесором [4].

Таким чином, GDPR – Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних є ключовим нормативним документом Європейського Союзу, який спрямований на захист персональних даних, причому його юридична дія поширюється і на українські компанії, які здійснюють обробку даних громадян держав-членів ЄС.

Безумовно, в умовах збільшення кількості випадків протиправного використання персональних даних, що становить пряму загрозу безпеці життєдіяльності кожної людини, дані якої протиправно розголошуються або використовуються, вищевказаний загальноєвропейський Регламент має пріоритетне значення для національних органів публічної адміністрації, які здійснюють адаптацію національного законодавства до права ЄС.

Не менш важливе значення для забезпечення безпеки життєдіяльності населення ЄС має Новий Регламент (ЄС) 2024/1689 від 13 червня 2024 року щодо штучного інтелекту [5].

Офіційний журнал Європейського Союзу опублікував Регламент (UE) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року, який встановлює гармонізовані правила щодо штучного інтелекту (англ. Artificial Intelligence Act, AI Act). Цей Закон є першим основним законодавчим актом у світі щодо штучного інтелекту. Проте вказаний Закон передбачає не лише контрольні та

регуляторні механізми, він також встановлює рекламні заходи (такі як регуляторні «пісочниці» та заходи для підтримки розвитку систем штучного інтелекту), спрямовані на заохочення розвитку технології щодо штучного інтелекту в соціальному плані [5].

Європейський закон про штучний інтелект зобов'язує держави-члени призначити один або декілька компетентних органів для нагляду за дотриманням зобов'язань, які він накладає. На європейському рівні Європейський офіс AI, створений Рішенням Комісії від 24 січня 2024 року (OJ-Z-2024-70007), буде наглядовим органом і матиме важливі функції, зокрема щодо нагляду за загальними моделями штучного інтелекту. Повноваження, які влада матиме для забезпечення ефективності Закону про AI, включають повноваження накладати штрафи. Штрафи за порушення Закону про штучний інтелект встановлюються у відсотках від річного обороту компанії-порушника за попередній фінансовий рік або заздалегідь визначеної суми, якщо вона вища та може зрости до 35 мільйонів євро або 7% від прибутку порушника зафіксованого в загальному світовому річному обороті за попередній фінансовий рік, якщо ця сума вища [5].

Даний Закон надає розробникам і користувачам систем чіткі вимоги та зобов'язання щодо конкретного використання штучного інтелекту, одночасно зменшуючи адміністративний і фінансовий тягар для бізнесу. Зобов'язання, передбачені вказаним Законом можуть стосуватися як постачальників (наприклад, розробника інструменту для перевірки резюме), так і користувачів систем штучного інтелекту (наприклад, банку, який купує цей інструмент перевірки) [6].

Закон про штучний інтелект запроваджує єдину структуру для всіх країн ЄС, засновану на далекоглядному визначенні штучного інтелекту та підході, заснованому на оцінці ризиків. Наприклад, системи штучного інтелекту, які дозволяють урядам або компаніям «оцінювати соціальні показники», вважаються явною загрозою основним правам людей і тому заборонені. Такими особливо шкідливими застосуваннями штучного інтелекту є: експлуатація вразливостей осіб, маніпулювання та використання підсвідомих прийомів; соціальний скоринг для державних і приватних цілей; індивідуальна предиктивна поліція, що ґрунтується виключно на профілюванні людей; нецілеспрямоване скрейпінг Інтернету або камер відеоспостереження для отримання зображень обличчя для створення або розширення баз даних; розпізнавання емоцій на робочому місці та в навчальних закладах, за винятком медичних причин або міркувань безпеки (наприклад, моніторинг рівня втоми пілота); біометрична категоризація фізичних осіб для визначення або визначення їхньої раси, політичних поглядів, членства в профспілках, релігійних чи філософських переконань або сексуальної орієнтації (маркування або фільтрація наборів даних та категоризація даних у сфері правоохоронних органів, як і раніше, будуть можливими); дистанційна біометрична ідентифікація в режимі реального часу в загальнодоступних місцях правоохоронними органами, за вузькими винятками [6].

Класифікація ризиків ґрунтується на цільовому призначенні системи штучного інтелекту, відповідно до чинного законодавства ЄС про безпеку продукції. Це означає, що класифікація залежить від функції, яку виконує система штучного інтелекту, а також від конкретної мети та способів, для яких використовується система. Системи штучного інтелекту можна віднести до категорії високого ризику у двох випадках: якщо система штучного інтелекту вбудована як компонент безпеки в продукти, на які поширюється чинне законодавство ЄС про безпеку продукції, або є самою такою продукцією (це може бути, наприклад, медичне програмне забезпечення на основі штучного інтелекту); якщо система штучного інтелекту призначена для використання в умовах високого ризику відповідно до Закону про штучний інтелект. Норми Закону включають

приклади використання штучного інтелекту в таких сферах, як освіта, працевлаштування, правоохоронні органи або міграція [6].

Таким чином, європейський закон про штучний інтелект (Artificial Intelligence Act, AI Act) є базовим правовим інструментом забезпечення безпеки життєдіяльності населення держав Європейського Союзу у суспільних відносинах, пов'язаних із використанням штучного інтелекту.

Складовою системи забезпечення безпеки життєдіяльності в Європейському Союзі є також забезпечення безпеки діяльності користувачів в інтернет-середовищі.

Так, О. Федотова зазначає, що у 2014 році Рада Європи затвердила спеціальну декларацію – Керівні принципи з прав людини для користувачів Інтернету у вигляді спеціальної Рекомендації Комітету Міністрів країнам-учасникам, згідно з якими їм належало: активно вживати заходів для захисту прав і свобод користувачів Інтернету, забезпечуючи повний доступ до послуг та ресурсів; регулярно оцінювати та усувати обмеження прав і свобод в Інтернеті, беручи до уваги той момент, що обмеження, передбачені законом, необхідні у демократичному суспільстві; забезпечувати доступ користувачів до ефективних правових механізмів у разі порушення їхніх прав, співпрацюючи з відповідними установами та структурами; сприяти налагодженню координації відповідних структур як всередині Ради Європи, так і поза нею, з метою впливу на стандарти та процедури захисту прав людини в Інтернеті; залучати приватний сектор до діалогу з державними органами та громадянським суспільством, сприяючи відповідальності підприємств перед суспільством та забезпечуючи прозорість їхньої діяльності [7, с. 85-86].

Також О. Федотова формулює висновок про те, що інформаційна політика ЄС формується з орієнтацію на захист діяльності користувачів в мережі Інтернет, про що безпосередньо свідчать загальноєвропейські правові документи. Задля забезпечення відповідності чинним європейським стандартам в інформаційній галузі, Україні потрібно виробити та застосувати на практиці ефективні інструменти, що зможуть в найкращий спосіб сприяти реалізації прав та свобод користувачів Інтернету [7, с. 86].

Окрему увагу необхідно також звернути на адаптацію національного законодавства, яке регулює суспільні відносини у сфері цивільного захисту, до відповідних положень права Європейського Союзу.

Так, О. Подскальна зазначає, що механізм цивільного захисту Європейського Союзу – найбільша в світі система надання міжнародної координованої оперативної допомоги при надзвичайних ситуаціях, яка включає різноманітні ресурси і форми допомоги. Рішення про заснування Механізму цивільного захисту Рада Європейського Союзу прийняла 23 жовтня 2001 року в м. Люксембурзі. З урахуванням набутого досвіду 17 грудня 2013 року Європейський парламент та Рада прийняли в м. Брюсселі Рішення № 1313/2013/EU «Про Механізм цивільного захисту Союзу» [8, с. 131].

Основна роль Механізму цивільного захисту полягає у сприянні співпраці у заходах з надання допомоги щодо захисту цивільного населення у разі настання надзвичайних ситуацій, які можуть вимагати прийняття термінових заходів реагування. Це відноситься і до ситуації, де може бути безпосередня загроза таких великих надзвичайних ситуацій. Механізм складається із ряду елементів і дій, що включають, у тому числі, і встановлення та управління центром моніторингу і інформації; встановлення і управління загальною аварійною системою зв'язку та інформації. Основною складовою, операційним ядром Механізму цивільного захисту є Координаційний центр реагування на надзвичайні ситуації, що діє під егідою Європейської комісії в м. Брюсселі, працює цілодобово без вихідних та надає країнам доступ до платформи цивільного захисту Європейського Співтовариства [8, с. 131].

Таким чином, в Механізмі цивільного захисту Європейського Союзу активно використовуються інформаційні технології, зокрема, інформаційні платформи, бази даних, засоби оперативного зв'язку. Відповідно, використання вказаних інформаційних технологій має належну правову регламентацію на рівні рішень Європейського парламенту та Європейської Ради.

Крім того, О. Подскальна справедливо зазначає, що розбудова сучасної та потужної системи цивільного захисту населення і територій України потребує ще більш тісної співпраці з відповідними європейськими структурами, зокрема в рамках Механізму цивільного захисту Європейського Союзу. Главою 6 «Навколишнє природне середовище» розділу 5 «Економічне і галузеве співробітництво» Угоди про асоціацію між Україною та Європейським Союзом передбачено співробітництво у сфері цивільного захисту [8, с. 133–134].

Реалізації одного із пріоритетів євроінтеграції – приєднання України до Механізму цивільного захисту Європейського Союзу сприятиме, на думку О. Подскальної, підписання та реалізація нової редакції Адміністративної домовленості між ДСНС України та Генеральним Директоратом «Навколишнє середовище» Європейської Комісії щодо співпраці між Координаційним центром реагування на надзвичайні ситуації Механізму цивільного захисту Співтовариства та Оперативно-черговою службою ДСНС України, подальша участь у заходах Фази 2 Програми Європейського Союзу з попередження, готовності та реагування на катастрофи природного та техногенного характеру для країн Східного партнерства (PPRD East) [8, с. 134].

Отже, враховуючи євроінтеграційні прагнення України, для органів публічної адміністрації нагальним є завдання завершити адаптацію національного законодавства в частині правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності до права Європейського Союзу.

Висновки. Проведене дослідження досвіду адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі дає підстави сформулювати висновок про те, що в Механізмі цивільного захисту Європейського Союзу використовуються такі інформаційні технології як інформаційні платформи, бази даних, засоби оперативного зв'язку та координації тощо. Використання вказаних інформаційних технологій має належну правову регламентацію на рівні рішень Європейського парламенту та Європейської Ради.

До правових засад використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід віднести GDPR – Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних, а також Європейський закон (Регламент) про штучний інтелект (Artificial Intelligence Act, AI Act).

Важливими документами щодо регулювання розвитку цифровізації в Європейському Союзі також є Європейська структура сумісності (EIF), яка надає загальний набір стандартів для забезпечення легкого доступу до державних послуг і спільного використання в усьому ЄС, а також Регламент eIDAS, що визначає правила електронної ідентифікації та довірчих послуг у всьому ЄС.

Враховуючи необхідність завершення процесів євроінтеграції, національним органам публічної адміністрації, зокрема Міністерству цифрової трансформації України, необхідно активізувати участь національних державних та приватних інституцій у розвитку Єдиного цифрового ринку ЄС, залучати інвестиції для розвитку національного цифрового ринку, включаючи фінансування заходів із забезпечення кібербезпеки. Крім того, одним із завдань є завершення процедур адап-

тації національного законодавства в частині правового регулювання використання інформаційних технологій та забезпечення безпеки життєдіяльності до права ЄС.

Анотація

Наукова публікація присвячена дослідженню досвіду адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі.

Зазначається, що однією з основних цілей функціонування єдиного цифрового ринку ЄС є посилення кібербезпеки та захист даних на території всього Європейського Союзу, що фактично є частиною системи забезпечення безпеки життєдіяльності громадян держав-членів ЄС. Одним із пріоритетів цифрової стратегії ЄС також є забезпечення безпечної цифрової інфраструктури, тобто фактично забезпечення безпеки життєдіяльності громадян ЄС в цифровому просторі та у суспільних відносинах, пов'язаних із використанням цифрових інструментів.

Серед правових засад використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності виділено GDPR – Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних, який є ключовим нормативним документом Європейського Союзу, що спрямований на захист персональних даних, причому його юридична дія поширюється і на українські компанії, які здійснюють обробку даних громадян держав-членів ЄС.

Також звернуто увагу на європейський закон (Регламент) про штучний інтелект (Artificial Intelligence Act, AI Act), який є базовим правовим інструментом забезпечення безпеки життєдіяльності населення держав Європейського Союзу у суспільних відносинах, пов'язаних із використанням штучного інтелекту.

Зазначається, що в Механізмі цивільного захисту Європейського Союзу активно використовуються інформаційні технології, зокрема, інформаційні платформи, бази даних, засоби оперативного зв'язку. Відповідно, використання вказаних інформаційних технологій має належну правову регламентацію на рівні рішень Європейського парламенту та Європейської Ради.

Формулюється висновок про те, що враховуючи євроінтеграційні прагнення України, для органів публічної адміністрації нагальним є завдання завершити адаптацію національного законодавства в частині правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності до права Європейського Союзу.

Ключові слова: зарубіжний досвід, правове регулювання, інформаційні технології, безпека життєдіяльності, персональні данні, штучний інтелект, цивільний захист, адаптація, гармонізація.

Bondar D.V. Experience of administrative and legal regulation of the use of information technologies in the field of ensuring the safety of life in the European Union

Summary

The scientific publication is devoted to the study of the experience of administrative and legal regulation of the use of information technologies in the field of ensuring the safety of life in the European Union.

It is noted that one of the main goals of the functioning of the single EU digital market is to strengthen cybersecurity and data protection throughout the European Union, which is actually part of the system for ensuring the safety of life of citizens of the EU Member States. One of the priorities of the EU digital strategy is also to ensure a secure digital infrastructure, that is, to ensure the safety of life of EU citizens in the digital space and in relations related to the use of digital tools.

Among the legal basis for the use of information technologies in the field of ensuring the safety of life, the GDPR – Regulation of the European Parliament and of the Council (EU) 2016/679 of April

27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, is highlighted, which is a key regulatory document of the European Union aimed at the protection of personal data, and its legal effect also extends to Ukrainian companies that process data of citizens of EU Member States.

Attention is also drawn to the European law (Regulation) on artificial intelligence (Artificial Intelligence Act, AI Act), which is the basic legal instrument for ensuring the safety of life of the population of the European Union in relations related to the use of artificial intelligence.

It is noted that the European Union Civil Protection Mechanism actively uses information technologies, in particular, information platforms, databases, and means of operational communication. Accordingly, the use of these information technologies has proper legal regulation at the level of decisions of the European Parliament and the European Council.

The conclusion is formulated that, taking into account Ukraine's European integration aspirations, it is an urgent task for public administration bodies to complete the adaptation of national legislation in terms of legal regulation of the use of information technologies in the field of ensuring life safety to the law of the European Union.

Key words: foreign experience, legal regulation, information technologies, life safety, personal data, artificial intelligence, civil protection, adaptation, harmonization.

Список використаних джерел:

1. Белова І., Ярощук О., Гомотюк А. Розвиток процесів цифровізації в Європейському Союзі: перспективний досвід для України. *Економічний аналіз.* 2023. Том 33. № 1. С. 180–191. DOI: https://doi.org/10.35774/econa2023.01.180
2. Цифрова стратегія ЄС. Проєкти EU4Digital. URL: https://eufordigital.eu/uk/discover-eu/eu-digital-strategy/ (дата звернення: 02.09.2024).
3. Положення ро Міністерство цифрової трансформації України, затверджене постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856. Дата оновлення: 01.06.2024. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text (дата звернення: 02.09.2024).
4. GDPR: захист персональних даних по-європейськи і чому це важливо? Mikhailenko Platform. URL: https://www.mikhailenko.com.ua/09-05-2023/gdpr-zahyst-personalnyh-danyh-po-yevropejsky-i-chomu-cze-vazhlyvo-2/ (дата звернення: 02.09.2024).
5. Новий Регламент (ЄС) 2024/1689 від 13 червня 2024 року щодо штучного інтелекту. Пахаренко і партнери: патентно-правова фірма. URL: http://pakharenko.ua/novij-reglament-yes-20241689-vid-13-chervnya-2024-roku-shhodo-shtuchnogo-intelektu/ (дата звернення: 02.09.2024).
6. Набув чинності Європейський закон про штучний інтелект. Про основні вимоги та зобов'язання при використанні штучного інтелекту. Liga zakon. URL: https://biz.ligazakon.net/analitycs/229699_nabuv-chinnost-vropeyskiy-zakon-pro-shtuchniy-ntelekt-pro-osnovn-vimogi-ta-zobovyazannya-pri-vikoristann-shtuchnogo-ntelektu (дата звернення: 02.09.2024).
7. Федотова О.О. Інформаційна політика ЄС із забезпечення безпеки діяльності користувачів в інтернет-середовищі. *Матеріали ІІІ Міжнародної науково-практичної конференції «Прикладні аспекти сучасних міждисциплінарних досліджень»* (м. Вінниця, 1 листопада 2024 р.). ДонНУ ім. Василя Стуса. С. 84–86. URL: https://jpasmd.donnu.edu.ua/article/view/16716 (дата звернення: 12.11.2024).
8. Подскальна О.А. Приєднання України до механізму цивільного захисту Європейського Союзу – один із пріоритетів її європейського вибору. *Інвестиції: практика та досвід.* 2015. № 19. С. 130–134.