УДК 342. 9
DOI https://doi.org/10.32782/2524-0374/2024-1/75

ЗАХИСТ ЦИФРОВОЇ ОСОБИСТОСТІ: ВИВЧЕННЯ ДОСВІДУ ЄВРОПЕЙСЬКОГО СОЮЗУ ТА УКРАЇНИ[1]

PROTECTION OF DIGITAL PERSONHOOD: STUDYING THE EXPERIENCE OF THE EUROPEAN UNION AND UKRAINE

Бондаренко О.С., д.ю.н., доцент,
завідувач кафедри кримінально-правових дисциплін та судочинства
Навчально-науковий інститут права Сумського державного університету

Думчиков М.О., к.ю.н., доцент,
старший викладач кафедри кримінально-правових дисциплін та судочинства
Навчально-науковий інститут права Сумського державного університету

Стаття присвячена важливій та актуальній темі особливостям захисту цифрової особистості в Європейському Союзі (далі – ЄС) та в Україні. У цифрову епоху відбувається обмін та обробка індивідуальних даних, які залишаються окремими складовими економічних та соціальних процесів. Ця особлива інформація має велике значення, адже цифровізація суспільства вимагає ефективного захисту цифрової особистості. Саме тому, у структурі цифрових прав громадян саме захист персональних даних є ключовим елементом, особливо в контексті кібербезпеки держави. Цифрова особистість представляє собою складову індивідуальності, що існує в онлайн середовищі. Цифрова особистість має значення в сучасному світі технологій, оскільки вона стала важливою складовою індивідуальної ідентичності в онлайн-середовищі. Зростання використання цифрових технологій, соціальних мереж, онлайн-сервісів та електронних платформ призвело до того, що багато аспектів життя людини стали відображатися в цифровому просторі. Порівняння цифрової особистості в ЄС та в Україні може включати декілька аспектів. Насамперед – це законодавство про захист персональних даних в ЄС та Україні. Так, в ЄС пакет документів стосовно захисту даних, прийнятий у травні 2016 року, має на меті зробити Європу придатною для цифрової ери. Другим аспектом, порівняння цифрової особистості в ЄС та в Україні є рівень використання технологій. У країнах ЄС високий рівень цифрової технологізації пов'язаний з широким використанням онлайн-сервісів, електронного урядування та інших інновацій. Третім аспектом порівняння цифрової особистості в ЄС та в Україні є доступ до високошвидкісного Інтернету. Четвертим аспектом порівняння цифрової особистості в ЄС та в Україні є цифрова грамотність. П'ятим аспектом порівняння цифрової особистості в ЄС та в Україні є кібербезпека. Порівнюючи досвід ЄС та України, стаття привертає увагу до ключових питань, таких як законодавча база, рівень освіченості населення щодо цифрової безпеки та заходи, спрямовані на захист особистих даних в Інтернеті. Захист цифрової особистості стає дедалі важливішим в контексті зростання кількості онлайн-загроз та використання особистих даних, особливо в умовах воєнного стану в Україні. Наголошується на важливості подальших заходів у вдосконаленні законодавства, збільшенні рівня свідомості населення та впровадженні ефективних технологічних рішень для захисту персональних даних.

Ключові слова: персональні дані, цифрова особистість, цифрова грамотність, кібербезпека, доступ до Інтернету, Європейський Союз, Загальний регламент захисту персональних даних (GDPR); Директива (ЄС) 2016/680, Закон про цифрові послуги.

The article is dedicated to the important and relevant topic of peculiarities in protecting digital identity in the European Union (EU) and Ukraine. In the digital era, the exchange and processing of individual data are integral components of economic and social processes. This specific information holds great significance, as societal digitization requires effective protection of digital identity. Therefore, within the framework of digital citizen rights, the safeguarding of personal data is a key element, especially in the context of state cybersecurity.

Digital identity constitutes a component of individuality existing in the online environment. It holds importance in today's technological world, becoming a crucial element of individual identity in the online realm. The increased use of digital technologies, social networks, online services, and electronic platforms has led to the reflection of many aspects of human life in the digital space.

A comparison of digital identity in the EU and Ukraine can include several aspects. Firstly, it involves legislation on personal data protection in the EU and Ukraine. The package of documents regarding data protection adopted in May 2016 aims to make Europe suitable for the digital era. Another aspect of comparing digital identity in the EU and Ukraine is the level of technology usage. In EU countries, a high level of digital technology integration is associated with widespread use of online services, e-governance, and other innovations. The third aspect of comparing digital identity in the EU and Ukraine is access to high-speed Internet. The fourth aspect is digital literacy, and the fifth aspect is cybersecurity.

By comparing the experiences of the EU and Ukraine, the article draws attention to key issues such as legislative frameworks, public awareness levels regarding digital security, and measures aimed at protecting personal data on the Internet. The protection of digital identity becomes increasingly crucial in the context of rising online threats and the use of personal data, especially in conditions of a state of war in Ukraine. The article underscores the importance of further legislative improvements, increasing public awareness, and implementing effective technological solutions for the protection of personal data.

Key words: personal data, digital identity, digital literacy, cybersecurity, internet access, European Union, General Data Protection Regulation (GDPR), Directive (EU) 2016/680, Digital Services Act.

Постановка проблеми. У цифрову епоху відбувається обмін та обробка індивідуальних даних, які залишаються окремими складовими економічних та соціальних процесів. Ця особлива інформація має велике значення, адже цифровізація суспільства вимагає ефективного захисту цифрової особистості. Саме тому, у структурі цифрових прав громадян саме захист персональних даних є ключовим елементом, особливо в контексті кібербезпеки держави. Вказане актуалізує необхідність вивчення особливостей захисту персональних даних в мережі Інтернет у контексті впровадження досвіду Європейського Союзу (далі – ЄС) у в українське законодавство.

Метою статті. Метою статті є характеристика особливостей захисту цифрової особистості в ЄС та в Україні в умовах воєнного стану.

Виклад основного матеріалу. Усвідомлення необхідності захисту цифрових прав в цілому та персональних даних в мережі Інтернет не є новим для сучасного періоду і, безумовно, не обумовлено воєнним станом. Кіберсередовище як та сфера, що в умовах діджиталізації активно розвивається стала об'єктом для злочинних посягань. Саме тому, виникла необхідність розроблення дієвого законодавства та конкретних механізмів захисту цифрової осо-

[1] Стаття написана в рамках проєкту Модуль Жана Моне «Досвід ЄС щодо захисту персональних даних у кіберпросторі» (2023–2026 – EUEPPDC – 101125350 – ERASMUS-JMO-2023-MODULE)

бистості. Досліджуючи цю тему, безперечно, необхідно розпочати з аналізу понятійно-категоріального апарату. Для досягнення цієї мети необхідно правильно розуміти кіберпростір та пов'язані з ним юридичні аспекти [1]. На думку М. Фурашев кібепростір представляє собою форму співіснування матеріальних та нематеріальних об'єктів та процесів, спрямованих на створення, сприйняття, запам'ятовування, обробку та обмін інформацією [2].

Особистість, безсумнівно, є однією з найбільш інтригуючих граней людських істот [3]. Цифрова особистість представляє собою складову індивідуальності, що існує в онлайн середовищі. Вона включає в себе різноманітні соціальні, інституційні, правові, наукові та технологічні аспекти, які необхідно розглядати для повного розуміння особистості в цілому.

S. Vogel виділяє п'ять видів цифрової особистості [4]:

1) відкрита цифрова особистість, яка переконана, що цифрові технології є хорошим способом взаємодії з друзями, клієнтами та партнерами;

2) сумлінна цифрова особистість – це та, що навряд чи спробує нову технологію, доки не буде продемонстровано її переваги;

3) екстраверт – сприймає нові технології та різноманітні методи спілкування з людьми, часто майже не замислюючись про наслідки, швидше за все, буде мікроблогером через Twitter або користувачем Facebook;

4) погодливі цифрові особистості використовуватимуть нові технології, оскільки вони оцінять переваги, які вони можуть принести, але можуть не максимізувати потенціал, оскільки вони хвилюються про те, щоб не набридати чи не заважати людям;

5) невротична цифрова особистість цинічно ставиться до нових технологій і схильна відкидати їх; їй навряд чи буде комфортно застосовувати соціальні мережі для ділових відносин.

Цифрова особистість має значення в сучасному світі технологій, оскільки вона стала важливою складовою індивідуальної ідентичності в онлайн-середовищі. Зростання використання цифрових технологій, соціальних мереж, онлайн-сервісів та електронних платформ призвело до того, що багато аспектів життя людини стали відображатися в цифровому просторі.

Наприклад, цифрова особистість визначає, як людина представляє себе в інтернеті, включаючи профілі в соціальних мережах, веб-сайти, коментарі, відгуки тощо. Компанії використовують цифрові дані для створення персоналізованого змісту та послуг, які відповідають індивідуальним потребам користувачів. Цифрова особистість використовується для електронної ідентифікації при доступі до різних сервісів та платформ. Онлайн-поведінка може впливати на репутацію особистості, оскільки багато рішень та вражень формуються на основі інформації, доступної в Інтернеті. У бізнесі цифрова особистість може визначати імідж фахівця, впливати на професійні можливості та сприяти розвитку мережевих контактів. Захист цифрової особистості стає критичним у зв'язку з ризиками кіберзлочинності, крадіжки особистих даних, атак на конфіденційність. Тому, зараз люди стають більш обізнаними щодо того, як їхні дані використовуються, і вимагають більшого контролю над своєю цифровою присутністю. У цілому, цифрова особистість стала невід'ємною частиною життя в інтернет-епоху, впливаючи на спосіб взаємодії людей, їхні можливості та ризики.

Порівняння цифрової особистості в ЄС та в Україні може включати декілька аспектів. Насамперед – це законодавство про захист персональних даних в ЄС. Пакет документів стосовно захисту даних, прийнятий у травні 2016 року, має на меті зробити Європу придатною для цифрової ери [5].

У структуру пакету нормативно-правових актів щодо захисту персональних даних входять: Регламент (ЄС) 2016/679 (Загальний регламент захисту персональних даних (GDPR); Директива (ЄС) 2016/680 про захист фізичних осіб щодо обробки персональних даних, пов'язаних із кримінальними правопорушеннями або виконанням кримінальних покарань, а також про вільний рух таких даних; Регламент (ЄС) 2018/1725 щодо обробки персональних даних установами, органами, офісами та агентствами Союзу; Закон про цифрові послуги (DSA).

Важливо зосередити увагу на кожному із цих документів. Загальний регламент ЄС із захисту персональних даних (далі – GDPR), який регулює, як персональні дані осіб у ЄС можуть оброблятися та передаватись, набув чинності 25 травня 2018 року. GDPR – це всеосяжне законодавство про конфіденційність, яке поширюється на всі сектори та компанії розміри. GDPR має широку сферу застосування та використовує широкі визначення. Компаніям, які не засновані в ЄС, доведеться дотримуватися Регламенту під час обробки персональних даних резидентів ЄС та ЄЕЗ, наприклад, у випадках, коли компанія пропонує товари чи послуги суб'єктам даних у ЄС або якщо компанія відстежує поведінку суб'єктів даних у межах ЄС. Як правило, компанії, засновані не в ЄС, але на які поширюється дія GDPR, повинні письмово призначити представника ЄС для забезпечення відповідності GDPR. Існує виняток із цієї вимоги для невеликого масштабу, випадкової обробки неконфіденційних даних. Штрафи у разі невиконання можуть сягати до 4% річного світового доходу або 20 мільйонів євро. Компанії будь-якого розміру та сектору мають розглядати GDPR як частину своїх загальних зусиль із забезпечення відповідності за допомогою юридичного радника [5].

Директива (ЄС) 2016/680 про захист фізичних осіб щодо обробки персональних даних, пов'язаних із кримінальними правопорушеннями або виконанням кримінальних покарань, а також про вільний рух таких даних захищає основоположне право громадян на захист даних, коли персональні дані використовуються кримінально-правовими органами для правоохоронних цілей. Це, зокрема, забезпечить належний захист особистих даних жертв, свідків і підозрюваних у злочинах і сприятиме транскордонному співробітництву в боротьбі зі злочинністю та тероризмом [5].

Регламент (ЄС) 2018/1725 щодо обробки персональних даних установами, органами, офісами та агентствами ЄС – це правовий акт ЄС, який регулює обробку персональних даних органами та установами ЄС. Регламент призначений для забезпечення високого рівня захисту фізичних осіб у зв'язку з обробкою їхніх персональних даних цими установами та органами. Він встановлює принципи чесності, законності, прозорості та інших засад для правильної обробки персональних даних. Гарантує права фізичних осіб щодо доступу до їхніх даних, виправлення помилок та видалення інформації. Регламент визначає ролі посадових осіб, які відповідають за внутрішній контроль та нагляд за дотриманням положень регламенту [7].

Закон про цифрові послуги є найважливішим і найамбітнішим у світі нормативним актом у сфері захисту цифрового простору від поширення незаконного контенту та захисту основних прав користувачів. У світі немає іншого законодавчого акту, який би мав такий рівень амбіцій щодо регулювання соціальних мереж, онлайн-ринків, дуже великих онлайн-платформ (VLOP) і дуже великих онлайн-пошукових систем (VLOSE). Правила розроблені асиметрично: більші посередницькі послуги зі значним суспільним впливом (VLOP і VLOSE) підпадають під більш суворі правила. Після прийняття Закону про цифрові послуги платформи не тільки повинні будуть бути більш прозорими, але й відповідатимуть за свою роль у поширенні незаконного та шкідливого контенту.

У контексті російського військового вторгнення в Україну, що супроводжується серйозними та широко

поширеними порушеннями прав людини українського народу, а також особливого впливу на маніпулювання онлайн-інформацією, Закон про цифрові послуги запроваджує механізм реагування на кризу. Цей механізм дозволить проаналізувати вплив діяльності VLOP та VLOSE на кризу та швидко прийняти рішення про пропорційні та ефективні заходи для забезпечення дотримання основних прав [8].

В Україні також прийнято законодавство щодо захисту особистих даних, але його рівень відповідності може відрізнятися від стандартів GDPR. Існує декілька ключових відмінностей між Законом України «Про захист персональних даних» та GDPR:

1) Україна прийняла Закон України «Про захист персональних даних» у 2010 році. Безперечно після цього до нього було внесено ряд змін і доповнень, однак в ньому досі відсутні положення про особливості захисту цифрової особистості, які враховуючи специфіку кіберсередовища, не можуть бути тотожними стандартним правилам захисту персональних даних. Натомість Регламент ЄС набрав чинності у 2018 році і застосовується безпосередньо до всіх країн-членів ЄС;

2) український закон визначає права та обов'язки суб'єктів даних, але не накладає на організації обов'язок призначення уповноваженої особи з питань захисту даних, натомість GDPR вимагає призначення уповноваженої особи з питань захисту даних для багатьох видів обробки даних, а також надає більше прав суб'єктам даних. Вказане є свідченням особливої уваги до захисту персональних даних особи, особливо з метою попередження привласнення собі чужої цифрової особистості та використання її у неправомірних цілях;

3) український закон встановлює адміністративні санкції за порушення правил обробки даних, а GDPR також надає органам нагляду великі повноваження щодо застосування адміністративних санкцій, включаючи значні штрафи. Тобто, прослідковується тенденція каральності у контексті попередження порушень захисту персональних даних.

Другим аспектом, порівняння цифрової особистості в ЄС та в Україні є рівень використання технологій. У країнах ЄС високий рівень цифрової технологізації пов'язаний з широким використанням онлайн-сервісів, електронного урядування та інших інновацій. Цифровий порядок денний для Європи служить рушієм цих стратегій для просування цифрових технологій у Європі. Європейська комісія розробила Індекс цифрової економіки та суспільства (DESI), який щорічно публікується з 2014 року для вимірювання та відстеження прогресу. Європейський парламент прийняв Цифровий порядок денний 2030: європейський метод досягнення Digital Decade [9, с. 430].

Так, запровадження бізнесом цифрових технологій має потенціал для покращення послуг і продуктів, а також підвищення конкурентоспроможності. Базовий рівень передбачає використання принаймні чотирьох із дванадцяти обраних цифрових технологій (наприклад, використання будь-якої технології штучного інтелекту; продажі електронної комерції становлять принаймні 1% від загального обороту тощо) [10].

Україна також активно розвиває цифрові технології, але рівень їхнього впровадження може бути різним. У 2023 році Міністерство цифрової трансформації за участю швейцарсько-української Програми EGAP, яка виконується Фондом Східна Європа, та компанією «Делойт» планує вперше провести оцінку рівня цифрових послуг та розвитку цифрової інфраструктури в територіальних громадах України. Для визначення ступеня цифровизації громад буде використано Базовий Індекс для малих та середніх територіальних громад та Розширений Індекс для великих громад, кожен з яких включає 5 блоків, об'єднаних, але з різним числом індикаторів – 65 та 78 відповідно [11].

Важливо акцентувати, що воєнний стан в Україні чинить суттєвий вплив на всі трансформаційні процеси. Зокрема, зменшення економічної стійкості країни може призвести до обмежень у фінансуванні ініціатив. Крім того, неминучі руйнування та пошкодження інфраструктури, включаючи ту, яка використовується для цифрових технологій. Відновлення та модернізація інфраструктури може вимагати значних зусиль та ресурсів. Військові дії можуть мати великий вплив на людські ресурси. Кадрові втрати в області технологій та інновацій можуть обмежити розвиток цифрових проєктів. Збройний конфлікт неминуче призводить до збільшення загроз в кіберпросторі. Кібератаки можуть стати складнішими і загрожувати безпеці цифрових систем. Саме тому, саме зараз для України є дуже важливим проведення цифрових реформ з орієнтацією на стандарти ЄС, однак і з врахуванням умов воєнного стану та важливості кібербезпеки як частини національної безпеки.

Третім аспектом порівняння цифрової особистості в ЄС та в Україні є доступ до високошвидкісного Інтернету. На думку L. Jasmontaite та P. De Hert доступ до Інтернету за своєю суттю є питанням управління Інтернетом, і тому його регулювання має спричинити обговорення багатьох зацікавлених сторін. Тоді доступ до Інтернету розглядатиметься не лише з технічного боку як послуга зв'язку, але як «набір пристроїв, послуг, засобів і навичок, які дозволяють людям підключатися до Інтернет-сервісів, програм і контенту та використовувати їх». Можливо, така зміна підходу може посилити роль ЄС у ширшому контексті управління Інтернетом [12].

Згідно зі щорічним звітом Global Digital Overview, станом на початок 2023 року інтернетом користувалися 5,16 млрд людей, а це приблизно 64% від населення Землі. При цьому серед міського населення інтернет-юзерів 78,3%, а серед сільського лише 45,8% [13].

Відповідно до даних, опублікованих Євростатом, минулого року близько 2,4% із 450 мільйонів жителів ЄС не могли дозволити собі підключення до Інтернету. Обнадійливим є те, що цей показник на 0,3% нижчий, ніж у попередньому році. Ця цифра зростає до 7,6%, якщо дивитися на людей, які вважаються групою ризику бідності. Частка загального населення та населення, яке перебуває під загрозою бідності та не може дозволити собі підключення до Інтернету, значно відрізняється в країнах ЄС. У Румунії у кожен четвертий із тих, хто перебуває на межі бідності, не міг дозволити собі підключення до Інтернету, а в Болгарії (20,5%) та Угорщині (16,5%) також зафіксовано високі частки. Найнижчі частки були зареєстровані в Данії та Фінляндії (обидві по 1,0%), за ними йдуть Кіпр і Люксембург (обидва по 1,5%) [14].

Україна також працює над розвитком доступу до Інтернету, але може існувати регіони з менш розвиненою інфраструктурою. Приблизно 82% населення України користується Інтернетом хоча б раз на тиждень, із них 78% роблять це щодня чи майже щодня, як свідчать результати опитування, проведеного Київським міжнародним інститутом соціології. Згідно з отриманими даними, міське населення використовує Інтернет частіше, ніж сільське, із зменшенням відсотка активних користувачів інтернету із зростанням віку. Використання Інтернету також зростає з рівнем освіти, і найменше його використовують українці віком 70+. Натомість, найбільше відсоток користувачів припадає на групу віком від 18 до 49 років. За гендерним розподілом можна зауважити, що приблизно однакова кількість чоловіків і жінок щодня або майже щодня використовують Інтернет [15]. Воєнні конфлікти можуть супроводжуватися припиненням електропостачання, що в свою чергу призводить до неможливості жителів та підприємств користуватися Інтернетом. У воєнний період можливі кібератаки на інфраструктуру та системи зв'язку, що може вплинути на якість і доступність Інтернет-послуг.

Четвертим аспектом порівняння цифрової особистості в ЄС та в Україні є цифрова грамотність. В ЄС робиться великий фокус на розвиток цифрової грамотності населення. Адже, цифрові навички є ключовим каталізатором успіху будь-якої цифрової трансформації, що дозволяє громадянам бути активними в цифровому суспільстві та підтримує економічне зростання шляхом впровадження нових технологій. У той час, коли попит на цифрові навички постійно зростає, цих навичок часто бракує [16].

Зараз у Європі кожен третій 13-річний учень не має базових цифрових навичок під час безпосереднього тестування, і, за даними ОЕСР, лише трохи більше половини 15-річних у ЄС повідомили, що їх навчали визначати, чи є інформація суб'єктивні чи упереджені. Отже, існує очевидна потреба посилити роль освіти та навчання в боротьбі з дезінформацією та просуванні цифрової грамотності, а також медіаграмотності. Це підвищить стійкість і можливість більш ефективно боротися з впливом онлайн-дезінформації [17].

У жовтні минулого року EU4Digital організував перший тренінг для України з управління національними коаліціями цифрових навичок і робочих місць. Програма, що фінансується ЄС, передбачає розробку нових методологій для оцінки рівня цифрових навичок серед населення та прогнозування дефіциту кваліфікованих кадрів на ринку, а також підтримала створення національної коаліції для розвитку цифрових навичок і роботи. створення в Україні.

Україна також визнає важливість цифрової грамотності. Відповідно до Програми діяльності Кабінету Міністрів України, затвердженої постановою Кабінету Міністрів України від 12 червня 2020 р. № 471, одним із пріоритетних завдань Уряду є цифрова грамотність українців, завдяки чому планується, що 6 млн українців зможе пройти програму цифрової грамотності. В умовах повномасштабної та гібридної інформаційної війни Росії проти України, громадянам необхідно активно протидіяти ворожій пропаганді, розвивати навички розпізнавання фейків та ефективно використовувати цифрові технології для забезпечення особистої безпеки та сприяння сталому розвитку. У період воєнного стану цифрові навички стають конкурентною перевагою, дозволяючи здобувати віддалену роботу, апскілінг та рескілінг. Розвиток цифрової грамотності сприятиме комфортнішому життю в Україні, надаючи можливість отримувати державні послуги онлайн та покращуючи якість життя через впевнене володіння соціальними мережами та Інтернетом [18].

П'ятим аспектом порівняння цифрової особистості в ЄС та в Україні є кібербезпека. Одне єдине порушення безпеки може призвести до розкриття особистої інформації мільйонів людей. Ці порушення мають сильний фінансовий вплив на компанії, а також втрату довіри клієнтів. Отже, кібербезпека дуже важлива для захисту компаній і окремих осіб від спамерів і кіберзлочинців.

Згідно з журналом Cybercrime Magazine, до 2025 року кіберзлочинність коштуватиме світові 10,5 трильйонів доларів щорічно! Крім того, прогнозується, що глобальні витрати на кіберзлочинність зростатимуть майже на 15 відсотків щорічно протягом наступних чотирьох років [19].

В ЄС високий рівень уваги приділяється кібербезпеці та захисту від кіберзагроз. Важливо відмітити, що загрози кібербезпеці майже завжди є транскордонними, а кібератака на критично важливі об'єкти однієї країни може вплинути на весь ЄС. Країни ЄС повинні мати сильні державні органи, які контролюють кібербезпеку в їхніх країнах і які співпрацюють зі своїми колегами в інших державах-членах, обмінюючись інформацією. Директива про безпеку мережевих та інформаційних систем (NIS Directive), яку зараз імплементували всі країни, забезпечує створення та співпрацю таких державних органів. Цю Директиву було переглянуто наприкінці 2020 року. У результаті процесу перегляду 16 грудня 2020 року Комісія представила пропозицію щодо Директиви про заходи для високого загального рівня кібербезпеки в Союзі (Директива NIS2). Директива була опублікована в Офіційному журналі ЄС в грудні 2022 року та набула чинності 16 січня 2023 року. Держави-члени матимуть 21 місяць з моменту набрання чинності Директивою, щоб включити положення до свого національного законодавства (фактично дата: 18 жовтня 2024 р.) [17].

В Україні також проводяться заходи щодо кібербезпеки. Державна служба спеціального зв'язку та захисту інформації України взяла на себе відповідальність за формування та реалізацію державної політики у сфері кіберзахисту, захисту критичної інфраструктури та державних інформаційних ресурсів у кіберпросторі в Україні [15]. Одним із напрямів такої політики є й впровадження стандартів ЄС.

Висновки. Порівнюючи досвід ЄС та України, стаття привертає увагу до ключових питань, таких як законодавча база, рівень освіченості населення щодо цифрової безпеки, та заходи, спрямовані на захист особистих даних в Інтернеті. Захист цифрової особистості стає дедалі важливішим в контексті зростання кількості онлайн-загроз та використання особистих даних, особливо в умовах воєнного стану в Україні. Наголошується на важливості подальших заходів у вдосконаленні законодавства, збільшенні рівня свідомості населення та впровадженні ефективних технологічних рішень для захисту персональних даних в мережі Інтернет.

ЛІТЕРАТУРА

1. Naseh M.V. Person and Personality in Cyber Space: A Legal Analysis of Virtual Identity. *SSRN Electronic Journal*. 2014. December 1. URL : 10.2139/ssrn.2532562 (date of access: 03.01.2024).

2. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2. URL : https://doi.org/10.37750/2616-6798.2012.2(5).271955 (дата звернення: 03.01.2024).

3. Picca D., Pitteloud J., Personality recognition in Digital Humanities: A review of computational approaches in the humanities, Digital Scholarship in the Humanities, 2023. fqad047. URL: https://doi.org/10.1093/llc/fqad047 (date of access: 03.01.2024).

4. Vogel S. Digital personality types – what's yours? *ZDNET* : website. URL: https://www.zdnet.com/article/digital-personality-types-whats-yours/ (date of access: 03.01.2024).

5. Data protection in the EU. *European Commission* : website. URL: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (date of access: 03.01.2024).

6. European Union – Data Privacy and Protection. *European Union Country Commercial Guide* : website. URL: https://www.privacyshield.gov/ (date of access: 03.01.2024).

7. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance). URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1725 (date of access: 03.01.2024).

8. The Digital Services Act (DSA). *Eu-digital-services* : website. URL : https://www.eu-digital-services-act.com/DiSeActTPro_Training.html (date of access: 03.01.2024).

9. Kovács T. Z., Nábrádi A., Bittner B. Digital Technology Integration Among Eastern European Companies, Based on Digital Economy and Society Index. *Interdisciplinary Description of Complex Systems*. 2023. № 21 (5). P. 421–440. https://doi.org/10.7906/ indecs.21.5.1

10. How digitalised are the EU's enterprises? Eurostat : website. URL : https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20220826-1 (date of access: 03.01.2024).

11. Мінцифра вперше виміряє рівень цифровізації у громадах: як це працюватиме. *Юридична газета онлайн* : вебсайт. URL : https://yur-gazeta.com/golovna/mincifra-vpershe-vimiryae-riven-cifrovizaciyi-u-gromadah-yak-ce-pracyuvatime.html (дата звернення: 03.01.2024).

12. Jasmontaite L. and De H., P. Access to the Internet in the EU: A Policy Priority, a Fundamental, a Human Right or a Concern for eGovernment? *BRUSSELS PRIVACY HUB WORKING PAPER*. 2020. VOL. 6. N 19. URL : https://ssrn.com/abstract=3535718 or http://dx.doi.org/10.2139/ssrn.3535718 (date of access: 03.01.2024).

13. Даниленко Ю., Миронович В. Скільки українців не мають доступу до інтернету і коли ми подолаємо цифровий розрив. *SPEKA* : вебсайт. URL : https://speka.media/skilki-ukrayinciv-dosi-ne-mayut-dostupu-do-internetu-i-shho-robiti-z-cifrovim-rozrivom-plg4x9 (дата звернення: 03.01.2024).

14. Millions in the EU still unable to afford internet. *Euronew :* website. URL : https://www.euronews.com/my-europe/2023/08/01/millions-in-the-eu-still-unable-to-afford-internet1(date of access: 03.01.2024).

15. Приблизно 82% українців користуються інтернетом хоча б раз на тиждень, із них 78% щодня чи майже щодня. Укрінформ : вебсайт. URL : https://www.ukrinform.ua/rubric-technology/3497671-blizko-78-ukrainciv-sodna-koristuutsa-internetom.html#:~:text=%D0%AF%D0%BA%20%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%94%20%D0%A3%D0%BA%D1%80%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%2C%20%D0%BF%D1%80%D0%BE%20%D1%86%D0%B5,78%25%20%D1%89%D0%BE%D0%B4%D0%BD%D1%8F%20%D1%87%D0%B8%20%D0%BC%D0%B0%D0%B9%D0%B6%D0%B5%20%D1%89%D0%BE%D0%B4%D0%BD%D1%8F. (дата звернення: 03.01.2024).

16. Ready for the digital decade? Improving skills to meet the technological challenge in Ukraine. *The EU4Digital Initiative :* website. URL : https://eufordigital.eu/ (date of access: 03.01.2024).

17. Commission steps up action to tackle disinformation and promote digital literacy among young people. *European Commission :* website. URL : https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6048 (date of access: 03.01.2024).

18. Одним із пріоритетних завдань Уряду є цифрова грамотність українців. URL : https://vclc.com.ua/news/%D0%BE%D0%B4%D0%BD%D0%B8%D0%BC-%D1%96%D0%B7-%D0%BF%D1%80%D1%96%D0%BE%D1%80%D0%B8%D1%82%D0%B5%D1%82%D0%BD%D0%B8%D1%85-%D0%B7%D0%B0%D0%B2%D0%B4%D0%B0%D0%BD%D1%8C-%D1%83%D1%80%D1%8F%D0%B4%D1%83-%D1%94/ (дата звернення: 03.01.2024).

19. Karin K. What is Cybersecurity and Why It is Important? *Simplilearn* : website. URL : https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security (date of access: 03.01.2024).