УДК 004.056
DOI https://doi.org/10.24144/2788-6018.2025.02.185

БЕЗПЕКА ІНФОРМАЦІЙНИХ МЕРЕЖ ТА ЗАХИСТ ПРАЙВЕСІ: ЕВРОПЕЙСЬКІ СТАНДАРТИ Й ІНТЕГРАЦІЙНІ ВИКЛИКИ ДЛЯ УКРАЇНИ

Мальцев С.Ю.,
аспірант кафедри міжнародного права
та права Європейського Союзу,
Державний податковий університет
ORCID: 0009-0000-5732-1989

Мальцев С.Ю. Безпека інформаційних мереж та захист прайвесі: європейські стандарти й інтеграційні виклики для України.

Стаття присвячена аналізу ключових категорій у сфері інформаційної безпеки та захисту приватності в умовах розвитку інформаційного суспільства й інтеграції України до Європейського Союзу. У роботі досліджено поняття «безпека інформаційних мереж», «інформаційне прайвесі» та «захист прайвесі в інформаційних мережах», які формують базис правового регулювання у цій сфері.

У статті розглянуто еволюцію понять інформаційної приватності та захисту приватності в інформаційних мережах, а також їх взаємозв'язок із категорією інформаційної безпеки, а також розглянуто виклики, пов'язані із застосуванням технологій штучного інтелекту, Big Data та Інтернету речей (IoT), які створюють нові загрози для приватності та вимагають розробки інноваційних підходів до захисту даних. Автор наголошує на важливості балансу між правами громадян на конфіденційність та потребами держави у сфері інформаційної безпеки, а також на необхідності розробки ефективних правових і технічних механізмів, здатних адаптуватися до сучасних загроз і викликів.

Основна увага приділена розвитку європейських стандартів захисту персональних даних, зокрема GDPR та ISO/IEC 27001, а також викликам, пов'язаним із забезпеченням конфіденційності, цілісності та доступності інформації в умовах цифровізації та глобалізації. У статті проаналізовано значення міжнародних стандартів, а також правових актів ЄС, які є основою для створення дієвої системи інформаційної безпеки та захисту приватності, з огляду на важливість впровадження цих норм в українське законодавство, що сприяє гармонізації правової бази України з acquis ЄС.

Результати дослідження спрямовані на формування стратегії правового захисту персональних даних у сучасному інформаційному середовищі, забезпечення надійності інформаційних мереж та дотримання прав людини.

Актуальність цього питання посилюється у контексті інтеграції України до ЄС, де впровадження європейських стандартів захисту приватності є важливою умовою для досягнення високого рівня інформаційної безпеки. Автор підкреслює, що інтеграція України до ЄС вимагає адаптації національного законодавства до європейських стандартів, що включає впровадження сучасних механізмів захисту персональних даних, підвищення рівня кібербезпеки та забезпечення прозорості в обробці інформації.

Стаття спрямована на формування стратегії правового захисту персональних даних у сучасному інформаційному середовищі, забезпечення надійності інформаційних мереж та дотримання прав людини в контексті євроінтеграції.

Ключові слова: інформаційна безпека, захист прайвесі, європейські стандарти, інформаційні мережі, персональні дані, євроінтеграція, конфіденційність, інформаційне суспільство.

Mal'tsev S.Yu. Information network security and privacy protection: European standards and integration challenges for Ukraine.

The article is dedicated to analyzing key categories in the field of information security and privacy protection in the context of the development of the information society and Ukraine's integration into the European Union. The study explores the concepts of «information network security,» «information privacy,» and «privacy protection in information networks,» which form the foundation of legal regulation in this domain.

The article examines the evolution of information privacy and privacy protection in information networks, as well as their relationship with the broader concept of information security. It also addresses challenges related to the application of artificial intelligence (AI), Big Data, and the Internet of Things (IoT), which introduce new threats to privacy and necessitate the development of innovative approaches to data protection. The author emphasizes the importance of balancing citizens' rights to

privacy with the state's needs in the field of information security, as well as the necessity of developing effective legal and technical mechanisms capable of adapting to modern threats and challenges.

Particular attention is given to the development of European standards for personal data protection, particularly the General Data Protection Regulation (GDPR) and ISO/IEC 27001, as well as the challenges associated with ensuring confidentiality, integrity, and availability of information in the context of digitalization and globalization. The article analyzes the significance of international standards and EU legal acts, which serve as the foundation for creating an effective system of information security and privacy protection. Special emphasis is placed on the importance of implementing these norms in Ukrainian legislation to harmonize Ukraine's legal framework with the EU acquis.

The research findings aim to contribute to the development of a legal strategy for personal data protection in the modern information environment, ensuring the reliability of information networks, and upholding human rights. The relevance of this issue is further heightened in the context of Ukraine's integration into the EU, where the implementation of European privacy protection standards is a crucial prerequisite for achieving a high level of information security. The author underscores that Ukraine's integration into the EU requires the adaptation of national legislation to European standards, including the implementation of modern mechanisms for personal data protection, enhancing cybersecurity levels, and ensuring transparency in information processing.

The article is focused on developing a legal strategy for personal data protection in the modern information environment, ensuring the reliability of information networks, and safeguarding human rights in the context of European integration.

Key words: information security, privacy protection, European standards, information networks, personal data, European integration, confidentiality, information society.

Постановка проблеми. У сучасному світі розвиток інформаційно-комунікаційних технологій (ІКТ) суттєво змінює підходи до регулювання інформаційної безпеки та захисту приватності. Ці питання стають особливо актуальними в умовах цифрової трансформації суспільства, глобалізації інформаційних потоків та зростання залежності держав, бізнесу і громадян від безпеки інформаційних систем.

Інтеграція України до Європейського Союзу зобов'язує адаптувати національне законодавство до європейських стандартів, зокрема в аспектах забезпечення інформаційної безпеки та захисту персональних даних. Угода про асоціацію між Україною та ЄС (яка вже є частиною національного законодавства) передбачає поступове наближення правової системи України до acquis ЄС, що включає впровадження Загального регламенту захисту даних (GDPR) та інших нормативних актів, спрямованих на забезпечення прав на конфіденційність та приватність [1, с. 97-98].

Водночас, стрімкий розвиток технологій створює нові виклики, пов'язані з безпекою інформаційних мереж, захистом персональних даних та використанням технологій штучного інтелекту, Big Data, Інтернету речей (IoT). Відсутність ефективних механізмів захисту може призвести до загроз приватності, витоків даних, зловживань та впливу на права людини.

У цьому контексті важливо сформулювати комплексне бачення таких категорій, як «інформаційна безпека», «інформаційне прайвесі» та «захист прайвесі в інформаційних мережах». Визначення цих понять та їхня роль у правовому регулюванні стають ключовими для розробки ефективних стратегій захисту у цифровому середовищі.

Таким чином, основна мета постановки питання – дослідити розвиток категорій інформаційної безпеки та захисту прайвесі з огляду на сучасні виклики та європейські стандарти у цій сфері, а також визначити інтеграційні виклики для України. Це дозволить окреслити стратегічні напрями адаптації українського законодавства та забезпечити високий рівень інформаційної безпеки в умовах євроінтеграції.

Метою статті є дослідження концептуальних засад безпеки інформаційних мереж, інформаційного прайвесі та захисту приватності в інформаційних мережах, які формують базис правового регулювання в цій сфері. Особливий акцент зроблено на дослідженні характеристик зазначених ключових категорій, а також історії питання, оскільки розуміння цих категорій в їх розвитку та пристосуванні до сучасних викликів є необхідною умовою для розробки та впровадження ефективної стратегії правового захисту в умовах сучасного інформаційного середовища у контексті гармонізації українського законодавства з європейськими стандартами.

Стан опрацювання проблематики. Питання сутності категорій «інформаційна безпека», «інформаційне прайвесі», а також міжнародно-правових стандартів у сфері захисту прайвесі в інформаційних мережах досліджували такі вітчизняні науковці, як Т.Ю. Ткачук, Б.А. Кормич, С.Л. Гнатюк, О.П. Горпинюк, О.Д. Довгань, А.Ю. Нашинець-Наумова, М.В. Баран, І.Р. Боднар, М.Т. Гаврильців, О.Г. Ярема, В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова та інші.

Попри значну кількість наукових праць у цій сфері, питання правового захисту прайвесі в інформаційних мережах у контексті інтеграції України до ЄС залишається дослідженим лише фрагментарно. Актуальним є подальший аналіз адаптації національного законодавства до acquis ЄС, імплементації європейських правових норм щодо цифрових прав і обов'язків суб'єктів, а також розробка ефективних механізмів забезпечення прайвесі з урахуванням сучасних викликів інформаційного суспільства. Зокрема, необхідно враховувати вплив таких технологічних феноменів, як штучний інтелект, великі дані (Big Data) та Інтернет речей (IoT), що суттєво змінюють парадигму захисту персональних даних та конфіденційності в цифровому середовищі.

Виклад основного матеріалу. Угода про асоціацію між Україною та Європейським Союзом (далі - Угода про асоціацію) закладає важливі основи для гармонізації українського законодавства із європейськими стандартами, зокрема у сфері інформаційного суспільства та електронних комунікацій. Стаття 394 Глави 14 Угоди про асоціацію «Інформаційне суспільство» визначає зобов'язання України забезпечити поступове наближення її правової системи до acquis ЄС у сфері регулювання інформаційних технологій, захисту персональних даних та приватного життя в інформаційних мережах.

В сучасному світі, в якому дедалі більшу роль у житті держави, її економіці та системі безпеки, відіграють кіберпростір та сучасні інформаційні технології, не можна обійти увагою ті загрози, які пов'язані з застосуванням цих високих технологій [2, с. 332]. Розвиток інформаційно-комунікаційних технологій (далі – ІКТ) створює нові можливості для суспільства, проте одночасно супроводжується низкою загроз, пов'язаних із забезпеченням безпеки інформаційних мереж та захистом права на прайвесі. У контексті інтеграції України до ЄС особливої актуальності набуває впровадження європейських стандартів захисту приватного життя в інформаційному просторі, які визначають високий рівень безпеки персональних даних, захищеність інформаційних мереж та відповідальність суб'єктів за порушення цих норм.

Тотальна комп'ютеризація телекомунікацій, систем транспортування, фінансів, обліку населення, медичного обслуговування, численних баз даних постійно збільшує кількість та якість інформації, що опрацьовується стосовно кожної особи, причому зазвичай без її відома. Існує та постійно вдосконалюється низка технологій для датамайнінгу та створення індивідуальних «онлайн-портретів» на основі збору та аналізу всіх відомостей, що мають будь-який (хай і непрямий) стосунок до користувачів. Рівень «деанонімізації» користувачів у сучасному онлайн-середовищі стає майже стовідсотковим, навіть якщо вони дотримуються вимог безпеки.

Якщо найближчим часом не буде знайдено ефективного й при цьому демократичного рішення проблеми захисту персональних даних у веб-середовищі, у перспективі це може призвести до непередбачуваних і небезпечних переосмислень загальноприйнятих уявлень про приватність, її сенс та межі [3, с. 53-54].

У цьому контексті виникає необхідність у поглибленому дослідженні та осмисленні категорій «безпека інформаційних мереж», «інформаційне прайвесі» та «захист прайвесі в інформаційних мережах».

Поняття «інформаційна безпека» тісно пов'язане з процесами інформатизації та формуванням інформаційного суспільства. Формуванню концепції інформаційної безпеки в контексті швидких технологічних змін, що впливають на суспільства, економіку та політику в глобальному вимірі, сприяли такі теоретики, як: Д. Белл, який у своїх працях описував перехід від індустріального суспільства до постіндустріального, де важливу роль відіграють інформаційні технології. Для нього інформація є важливим ресурсом, і її безпека стає критичним аспектом у контексті нового інформаційного порядку (*«The Coming of Post-Industrial Society: A Venture in Social Forecasting»* (1973). Е. Тоффлер також акцентував увагу на трансформаціях, які відбуваються в суспільствах через технологічні зміни, зокрема через розвиток інформаційних технологій. Він визначав інформаційну революцію як фундаментальний перехід у способах обробки та передачі інформації, що сприяє появі нових загроз для безпеки (*«Future Shock»* (1970), *«The Third Wave»* (1980)). Т. Стоуньер наголошував на необхідності вивчення соціальних та культурних аспектів інформатизації, що має важливе значення для захисту особистої інформації та визначення нових моделей безпеки в інформаційному суспільстві (*«The Third Industrial Revolution: How Lateral Power Is Transforming Energy, the Economy, and the World»* (2013)). А. Турен підкреслював, що в епоху інформації питання безпеки є не лише технологічним, але й політичним і соціальним, оскільки доступ до інформації може використовуватися для маніпулювання масовими уявленнями та управління суспільними процесами (*«The Post-Sovereign Condition: The International Legal System and the Limits of the State»* (2002)). М. Кастельс ввів концепцію «мережевого суспільства», де інформаційна безпека є не лише питанням захисту даних, а й впливу нових технологій на структуру та взаємодію суспільства (*«The Rise of the Network Society»* (1996), *«Communication Power»* (2009)). К. Кояма фокусувався

на аспектах правового регулювання і захисту в умовах інформаційної революції, визначаючи нові виклики для держав та міжнародних організацій у забезпеченні безпеки в інформаційних системах (*«Information and the Role of the State in the Modern Economy»* (2003)). Є. Масуда розглядав інформацію як критичний елемент розвитку суспільства і одночасно джерело потенційних загроз, що потребує нових підходів до її захисту на глобальному рівні (*«The Information Society as Post-Industrial Society»* (1980)). Н. Негропонте бачив інформаційне суспільство як суспільство, де цифрові технології є інтегрованою частиною повсякденного життя, описував перехід від аналогового світу до цифрового і прогнозував, як ці зміни вплинуть на наше життя («Being Digital» (1995).

У науковій літературі відсутній єдиний усталений погляд на зміст поняття «інформаційна безпека». Існує необхідність уточнення поняття інформаційної безпеки, яке сприятиме осмисленню перспективних змін інформаційної безпеки та дозволить повніше розкрити її зміст та надання йому більш широкого й системного характеру [4, с. 6].

Найбільш широкі підходи відображають не тільки технічний та управлінський аспекти поняття «інформаційна безпека», а й визначають системний, політичний, правовий і соціальний спектр інформаційної безпеки як явища, дозволяють розглядати інформаційну безпеку як інтегральне явище, що включає аспекти, необхідні для сталого розвитку суспільства й держави, як то: 1) стан захищеності інформаційного простору – загальне визначення, що охоплює всі аспекти захисту інформаційного середовища; 2) процес управління загрозами – відображає динамічний характер безпеки, орієнтований на управління ризиками; 3) захищеність національних інтересів – прив'язує інформаційну безпеку до стратегії національної безпеки; 4) нормативний захист – акцентує увагу на правовому регулюванні інформаційних процесів; 5) соціальні відносини – підхід, який враховує інтереси особистості, суспільства і держави; 6) функція держави – вказує на відповідальність держави за забезпечення безпеки; 7) складова національної безпеки – підкреслює значення інформаційної безпеки у глобальних стратегіях країни.

Наприклад, В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова визначають інформаційну безпеку у найзагальнішому випадку як стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави, а розгорнуте формулювання інформаційної безпеки, на думку зазначених авторів – це стан захищеності потреб в інформації особи, суспільства й держави, за якого забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [4, с. 11-12].

На думку Кононенка В., Здодовко С., на міжнародному рівні стан інформаційної безпеки передбачає захист від інформаційного впливу на свідомість суспільства та прийняття рішень державами та міжнародними організаціями, а також недоторканість приватних, державних та міжнародних цифрових баз даних, можливість їх швидкого відновлення у випадку протиправного посягання і забезпечення покарання суб'єктів таких посягань [5, с. 248-249].

Для визначення змісту та суті категорії «інформаційна безпека» в суто технічно-управлінському аспекті, в якому на думку автора ця категорія пов'язана із категорією «захисту прайвесі в інформаційних мережах» доцільно звернутися до міжнародного стандарту ISO/IEC 27001 Інформаційні технології – Методи захисту – Системи управління інформаційною безпекою – Вимоги, який визначає вимоги до створення, впровадження, функціонування, моніторингу, підтримки та вдосконалення системи управління інформаційною безпекою (СУІБ).

У стандарті ISO/IEC 27001 інформаційна безпека визначається через три основні аспекти:

1. Конфіденційність (Confidentiality) – забезпечення того, щоб доступ до інформації був лише у тих осіб чи систем, яким це дозволено. Це запобігає несанкціонованому доступу або розголошенню інформації.
2. Цілісність (Integrity) – гарантування, що інформація є точною, повною та незмінною, а також захищеною від несанкціонованих змін чи пошкоджень.
3. Доступність (Availability) – забезпечення того, щоб інформація була доступною та використовуваною в разі потреби для авторизованих користувачів, без затримок, перебоїв чи іншого впливу, що може знизити ефективність.

Таким чином з міжнародним стандартом ISO/IEC 27001, поняття інформаційної безпеки визначається як захист інформації від низки загроз, щоб забезпечити її конфіденційність, цілісність і доступність.

ISO/IEC 27001 також вказує, що інформаційна безпека не є лише технічним питанням, а повинна бути інтегрована в загальну бізнес-стратегію організації. Це передбачає створення структурованої політики безпеки, оцінку ризиків, визначення та застосування контрольних механізмів для забезпечення захисту інформаційних активів.

Питання забезпечення інформаційної безпеки є надзвичайно важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяг-

ганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу [6, с. 353].

Визначення поняття «інформаційна безпека» зі стандарту ISO/IEC 27001 може братися за основу при дослідженні категорії «захисту прайвесі в інформаційних мережах» з кількох причин:

– використання визначення зі стандарту ISO/IEC 27001 дає можливість забезпечити відповідність досліджень та практик міжнародним вимогам, що особливо важливо для інтеграції України до європейського та глобального інформаційного простору.

– концепція інформаційної безпеки, закладена в ISO/IEC 27001, узгоджується з європейськими та міжнародними нормативними актами, такими як Загальний регламент захисту даних (GDPR), що є важливим у контексті євроінтеграції України.

Таким чином, визначення інформаційної безпеки зі стандарту ISO/IEC 27001 є базовим і зручним для дослідження, оскільки відображає сучасні підходи до захисту інформації, легко адаптується до різних умов, дозволяє зосередити увагу на аналізі специфічних норм та вимог ЄС у сфері інформаційної безпеки та захисту прайвесі, а також визначити проблеми, з якими стикається Україна при інтеграції до ЄС.

Інформаційне прайвесі в узагальненому вигляді - це право особи на контроль за використанням її персональних даних та збереження приватності в інформаційних мережах. В інформаційному суспільстві інформаційна привітність стає фундаментальним правом кожної людини, вона охоплює право особи на те, щоб вирішувати, які саме дані про неї збираються інформаційних мережах, зберігаються, використовуються і розповсюджуються.

Поняття інформаційної приватності є динамічним і постійно еволюціонує у відповідь на стрімкий розвиток технологій, зростання обсягів обробки даних та їхнього використання в різних сферах суспільного життя. Зі зміною цифрового середовища, способів комунікації та форм обміну інформацією, концепція інформаційної приватності розширюється, включаючи нові аспекти захисту даних, персональної ідентифікації, а також прав людини в умовах інформаційного суспільства.

Якщо раніше приватність асоціювалася з фізичним простором – нашим будинком, особистим життям, яке було недоступне для сторонніх очей, то сьогодні це поняття розширилося і охоплює наш цифровий слід. Кожен наш крок в інтернеті залишає сліди – від відвідування веб-сайтів до покупок онлайн. Ці дані збираються, зберігаються і часто використовуються в комерційних цілях або для аналізу поведінки користувачів.

Д. Солов підкреслює, що якщо ми не переосмислимо бінарне уявлення про приватність, нові технології все більше і більше вторгатимуться в оазиси приватності, якими ми користуємося на публіці. Приватність – це складний набір норм, очікувань та бажань, який значно перевищує спрощене уявлення про те, що якщо ви на публіці, у вас немає приватності. Д. Солов розглядає приватність як соціальну цінність, оскільки приватність не є абстрактною концепцією, а має реальні соціальні наслідки, її захист необхідний для збереження демократії, свободи слова та особистої гідності [7, с. 166].

Зміна концептуальних підходів у розумінні інформаційної приватності відбувалася в наступні умовні етапи:

1. Відсутність поняття приватності в цифровому світі.

З появою перших комп'ютерів і мереж, питання приватності не стояло настільки гостро. Інформація була розподілена, а доступ до неї був обмежений.

2. Розуміння приватності як аналогу фізичної.

З розвитком Інтернету почали виникати перші спроби перенести поняття приватності з фізичного світу в цифровий. Виникла потреба в захисті особистої інформації від несанкціонованого доступу.

3. Формування концепції інформаційної приватності.

З появою соціальних мереж, електронної комерції та інших онлайн-сервісів, поняття приватності стало більш складним і багатогранним. Виникла потреба в розробці нових юридичних і технічних засобів захисту персональних даних.

4. Глобалізація проблеми приватності

Зростання глобалізації та інтеграції інформаційних систем призвело до того, що питання приватності стало міжнародною проблемою. Були розроблені міжнародні договори та стандарти, що регулюють захист персональних даних.

Еволюція поняття інформаційної приватності демонструє перехід від простого фізичного захисту особистих даних до комплексного підходу, який охоплює правові, технічні та етичні аспекти. Це робить інформаційну приватність ключовим елементом безпечного та справедливого цифрового суспільства.

Сучасне поняття «інформаційне прайвесі» можна визначати різними способами залежно від контексту: правового, технологічного, соціального чи етичного.

В юридичному аспекті інформаційне прайвесі – це право особи на захист її особистої інформації, яка обробляється, зберігається або передається у цифрових та неділжиталізованих середовищах, від незаконного збору, використання або розкриття.

В технологічному аспекті інформаційне прайвесі визначається як стан, за якого технічні системи забезпечують конфіденційність, цілісність і доступність персональної інформації та механізми її захисту від несанкціонованого доступу чи зловживання.

Соціальний аспект розкриває інформаційне прайвесі як суспільні відносини, що забезпечують захист права людини на приватне життя в умовах глобалізації інформаційних потоків та цифровізації.

В етичному аспекті інформаційне прайвесі – це моральне право особи на контроль над тим, які аспекти її особистої інформації стають доступними для інших, та обмеження у використанні цієї інформації.

Якщо розглядати інформаційне прайвесі в глобальному вимірі - це частина права на приватність, яке є універсальним правом людини, визнаним міжнародними договорами, що охоплює захист даних в електронних системах обміну інформацією.

Поведінковий підхід характеризує інформаційне прайвесі як здатність особи самостійно визначати межі, способи та обсяг розкриття своїх персональних даних у взаємодії з іншими суб'єктами.

В економічному аспекті інформаційне прайвесі можна розглядати як право особи на захист її персональних даних як нематеріального активу, що має економічну цінність.

Горпинюк О.П. визначає такі ознаки інформаційної приватності:

- Інформаційна приватність – це завжди інформація про певну частину життєдіяльності, яка для кожного індивідуальна.
- За змістом інформаційна приватність охоплює найрізноманітніші види інформації, які мають бути позбавлені публічного чи суспільного інтересу.
- Залежно від засобів зв'язку, за допомогою яких передається інформація, інформаційна приватність охоплює відомості, що передаються найрізноманітнішими засобами комунікацій. Водночас подати вичерпний перелік засобів зв'язку, за допомогою яких передається інформація, неможливо. Уже зараз можна прогнозувати, що з часом з'являтимуться нові технічні можливості для передачі інформації [8, с. 29–36].

У взаємозв'язку із категоріями «інформаційна безпека» та «захист прайвесі в інформаційних мережах», на думку автора статті, доцільно використовувати визначення «інформаційного прайвесі», яке відображає баланс між захистом інформації, управлінням ризиками безпеки та забезпеченням прав особи на приватність у цифровому середовищі. Інформаційна безпека зосереджена на захисті даних від загроз (конфіденційність, цілісність, доступність), а інформаційне прайвесі додає акцент на права людини, враховуючи етичні та правові аспекти. Захист прайвесі в мережах стосується дотримання прав на конфіденційність у контексті обробки даних у мережевих середовищах, а інформаційне прайвесі забезпечує інтеграцію цих прав у ширшу систему захисту інформації.

Таким чином, у взаємозв'язку із вищезазначеними категоріями варто розглядати інформаційне прайвесі як стан захищеності персональної інформації особи, що забезпечується через заходи інформаційної безпеки, механізми управління ризиками у мережах і технологіях, а також юридичні та технічні гарантії, спрямовані на збереження конфіденційності, цілісності та доступності даних, які перебувають в інформаційних системах і мережах.

Важливість категорії «Захист прайвесі в інформаційних мережах» очевидна в умовах стрімкого розвитку інформаційно-комунікаційних технологій (ІКТ) та постійних змін у кіберпросторі.

Майже в усіх країнах і міждержавних об'єднаннях найбільш проблемною сферою захисту ПД сьогодні є ІТ і кіберпростір як нове специфічне інформаційно-комунікаційне середовище, що стрімко розвивається і збільшується. У цій сфері нормативно-правове регулювання хронічно відстає від якісного (технології) та кількісного (пропускна здатність і поширеність інфраструктур) розвитку. Це відставання окреслилося ще у 80–90-х роках XX ст., але стало дійсно системною проблемою протягом 2000-х років разом із появою революційних винаходів та змінами в інформаційно-комунікаційних технологіях (ІКТ), лавиноподібним розширенням Всесвітньої мережі і міграцією цілих сфер людської діяльності в онлайн-сектор. Виникло й продовжує швидко зростати цілком нове, унікальне середовище, в якому традиційні нормативно-правові механізми, практики та підходи щодо захисту персональних даних стають здебільшого неефективними [3, с. 7-8].

Категорії «Інформаційна приватність» та «захист приватності в інформаційних мережах» тісно пов'язані поняття, які описують різні аспекти одного й того ж явища – права людини на контроль над своєю особистою інформацією в цифровому світі.

Якщо інформаційна приватність є метою, то захист приватності в інформаційних мережах – це засіб досягнення цієї мети.

Основний законодавчий акт, який з моменту його введення в дію 25 травня 2018 року став новим стандартом для захисту приватності та прав осіб у цифровому світі Інтернету та який регулює збір, зберігання, обробку та передачу персональних даних громадян ЄС – Загальний регламент про захист даних (GDPR), надає визначення «порушенню захисту персональних даних»: це порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, які передано, збережено або іншим чином опрацьовано. Саме недопущення випадкового чи незаконного знищення, втрати, зміни, несанкціонованого розкриття або доступу до інформації, яка входить в категорію «інформаційна приватність» - і є основною метою такої категорії, як «захист приватності в інформаційних мережах».

Коли ми говоримо про інформаційну приватність, ми маємо на увазі наше право не розголошувати свою особисту інформацію, наприклад, адресу, номер телефону чи історію пошуку. Захист приватності в інформаційних мережах – це комплекс заходів, таких як шифрування даних, створення захищених паролів, використання антивірусних програм, які допомагають забезпечити це право.

Розуміння взаємозв'язку між цими поняттями допомагає усвідомити ризики, пов'язані з використанням інформаційних технологій, і вживати необхідних заходів для їх мінімізації.

Як і категорія інформаційної приватності, поняття захисту приватності в інформаційних мережах безпосередньо пов'язане з прогресом інформаційних технологій і процесами глобалізації, що зумовлює його динамічний характер. З розвитком цифрових комунікацій і збільшенням обсягу обробки персональних даних у глобальних мережах це поняття зазнає постійних змін, пристосовуючись до нових викликів і ризиків.

З одного боку, сучасні технології створюють можливості для ефективного управління персональними даними, використання яких може покращити якість життя та спростити доступ до послуг. З іншого боку, глобалізація інформаційних потоків та швидкий обмін даними між країнами створюють нові загрози, зокрема несанкціоноване використання, порушення конфіденційності або контроль з боку держав чи корпорацій.

Поняття захисту приватності в інформаційних мережах зазнало значної еволюції, починаючи з моменту появи перших комп'ютерів. З розвитком інформаційних технологій, зміною соціальних норм та стрімким зростанням залежності сучасного суспільства від цифрових інструментів, стало очевидним, що традиційні підходи до забезпечення конфіденційності є недостатніми.

Із кожним етапом розвитку цифрових технологій нові ризики і загрози для приватності вимагали створення більш складних та всеосяжних механізмів захисту персональних даних. Це зумовило необхідність розробки нормативних актів, впровадження міжнародних стандартів і технологічних рішень, які враховують як технічні, так і правові аспекти інформаційної безпеки.

Таким чином, поняття захисту приватності в інформаційних мережах є не тільки технічним, але й правовим та соціальним явищем. Воно включає розробку та впровадження ефективних механізмів для дотримання балансу між правом на приватність та потребою вільного обміну інформацією в умовах глобалізованого інформаційного суспільства.

Поняття захисту приватності в інформаційних мережах в умовах глобалізації та інтеграції цифрових мереж, на думку автора статті, варто визначати як сукупність правових, технічних, організаційних та етичних заходів, спрямованих на забезпечення конфіденційності, цілісності, доступності та контролю над персональною інформацією, що обробляється, передається або зберігається у цифровому середовищі, з урахуванням міжнародних стандартів і прав людини.

Це поняття охоплює гарантування прав суб'єктів даних на конфіденційність та захист від незаконного втручання; впровадження нормативно-правових механізмів, таких як GDPR, для встановлення чітких правил обробки персональних даних; реалізацію технічних рішень (шифрування, анонімізація, багаторівнева автентифікація), що забезпечують безпеку інформації; міжнародну співпрацю в галузі кібербезпеки для координації зусиль щодо протидії глобальним загрозам; етичний підхід до збирання та використання даних у відповідності до принципів прозорості та згоди.

Таке визначення враховує складність сучасних викликів, пов'язаних із стрімким розвитком цифрових технологій, та акцентує на балансі між забезпеченням інновацій і захистом прав людини.

Україна, прагнучі до європейської інтеграції, стикається з низкою викликів у сфері імплементації та гармонізації європейських стандартів безпеки інформаційних мереж та захисту приватності. Ці виклики зумовлені як внутрішніми факторами (стан законодавства, рівень кібербезпеки, обізнаність населення), так і зовнішніми (швидкий розвиток технологій, глобалізація кіберзагроз).

Стосовно гармонізації в аспекті євроінтеграції – це взаємозближення правових систем національного законодавства та права ЄС, яку можна розділити на три складники: імплементація конкретних міжнародних норм, апроксимація транснаціональних нормативних положень та адаптація законодавства загалом [9, с. 11].

Імплементація європейських стандартів безпеки інформаційних мереж та захисту приватності в Україні є складним процесом, який вимагає комплексних заходів. Для успішної реалізації цієї мети необхідно залучати зусилля держави, бізнесу, громадянського суспільства та міжнародних партнерів.

Ускладнює процес інтеграції й перебування України в стані постійної кіберзагрози з боку іноземних держав, що має враховувати специфічні ризики та необхідність адаптації європейських стандартів до наших реалій.

Крім того, важливим викликом залишається традиційно низький рівень довіри населення до державних інституцій у сфері захисту даних. Європейські стандарти вимагають високого рівня прозорості, що потребує реформування системи управління інформаційною безпекою.

Ці виклики можуть бути вирішені за рахунок тісної співпраці з європейськими партнерами, залучення міжнародної допомоги та активної участі держави, приватного сектору та громадянського суспільства в реалізації відповідних реформ.

Висновки. У статті досліджено ключові категорії, що формують основу правового регулювання інформаційної безпеки та захисту приватності: «безпека інформаційних мереж», «інформаційне прайвесі» та «захист прайвесі в інформаційних мережах». Ці поняття розглядаються як взаємопов'язані елементи, які забезпечують конфіденційність, цілісність та доступність інформації, а також захищають права особи на контроль над своїми персональними даними.

Особливу увагу приділено європейським стандартам, зокрема GDPR та ISO/IEC 27001, які визначають високі вимоги до захисту персональних даних та інформаційної безпеки. Впровадження цих стандартів є ключовим елементом гармонізації українського законодавства з acquis ЄС. Це не лише сприяє інтеграції України до європейського інформаційного простору, але й формує довіру до цифрової екосистеми країни.

Для забезпечення інформаційної безпеки та захисту приватності на фоні стрімкого розвитку інформаційно-комунікаційних технологій та виникнення нових загроз для інформаційної безпеки та приватності необхідно впроваджувати комплексні підходи, які включають правові механізми (гармонізація національного законодавства з європейськими стандартами, впровадження GDPR, розробка нових нормативних актів), технічні заходи (шифрування даних, анонімізація, багаторівнева автентифікація, системи управління інформаційною безпекою, тощо), та організаційні заходи (зокрема підвищення обізнаності населення, навчання фахівців, створення ефективних механізмів реагування на кіберзагрози).

Для успішної інтеграції України до ЄС та його інформаційного простору, а також для забезпечення високого рівня інформаційної безпеки з огляду на існуючі виклики, такі як недосконалість законодавства, кіберзагрози, низький рівень довіри населення державним інституціям у сфері захисту даних, необхідно розробити стратегію правового захисту персональних даних, яка враховуватиме сучасні виклики та тенденції розвитку міжнародних стандартів, забезпечити баланс між правами громадян і потребами держави у сфері інформаційної безпеки, а також активно співпрацювати з європейськими партнерами для обміну досвідом та отримання технічної допомоги.

Результати дослідження підкреслюють важливість чіткого визначення та розуміння категорій інформаційної безпеки та захисту приватності для формування ефективної правової бази, що дозволяє не лише протистояти сучасним загрозам, але й забезпечувати сталий розвиток інформаційного суспільства в Україні в умовах євроінтеграції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кононенко В.П. Законодавство чи закон? *Право України*. 2004. № 4. С. 96–98.
2. Тимченко Л.Д., Кононенко В.П. Міжнародне право: підручник. К.: Знання, 2012. 631 с.
3. Гнатюк С.Л. Особливості захисту персональних даних у сучасному кіберпросторі: правові та техніко-технологічні аспекти: аналіт. доп. К.: НІСД, 2014. 92 с.
4. Інформаційна безпека держави: навч. посіб. / Гур'єв В.І., Мехед Д.Б., Ткач Ю.М., Фірсова І.В. Ніжин, 2018. 166 с.
5. Кононенко В.П., Здоровко С.С., Корольова А.Є. Інформаційна безпека як стан. *Науковий вісник Ужгородського національного університету*. Серія Право. 2023. № 76. Ч. 2. С. 244–250. DOI: https://doi.org/10.24144/2307-3322.2022.76.2.39.
6. Кононенко В.П., Новікова Л.В., Копицька П.О. Політика міжнародних організацій з питань інформаційної безпеки. *Науковий вісник Ужгородського національного університету*. Серія Право. 2021. № 65. Т. 1. С. 353–358. DOI: https://doi.org/10.24144/2307-3322.2021.65.64.
7. Solove, Daniel J. The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. *Yale University Press*. 2007. 257 с. URL: https://ssrn.com/abstract=2899125.

8. Горпинюк О.П. Інформаційна приватність та її захист від злочинних посягань в Україні: монографія. Львів: Видавництво «БОНА», 2014. 324 с.
9. Бондаренко О.С., Малетов Д.В. Гармонізація ІТ-права України в правом ЄС. *Південноукраїнський правничий часопис.* 2022. № 4. С. 9–16. DOI: https://doi.org/10.32850/sulj.2022.4.1.2.