УДК 004.056.53
DOI: https://doi.org/10.30838/EP.197.212-216

Похідня Б.А.
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Pokhidnia Bohdan
National University «Yuri Kondratyuk Poltava Polytechnic»

ЕТИКА В ІНФОРМАЦІЙНОМУ МЕНЕДЖМЕНТІ: ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

У статті досліджено етичні аспекти інформаційного менеджменту у сфері захисту персональних даних. Особливу увагу приділено сучасним викликам у сфері інформаційної безпеки, зокрема кіберзагрозам, проблемам конфіденційності, етичним аспектам використання алгоритмів та нормативно-правовим механізмам захисту даних. Проаналізовано міжнародні стандарти, такі як GDPR, ISO/IEC 27001, а також підходи до корпоративної етики в управлінні інформаційними ресурсами. Наведено рекомендації щодо вдосконалення механізмів захисту персональних даних, використання технологій шифрування та посилення відповідальності організацій за безпеку інформації. У статті розглянуто етичні аспекти інформаційного менеджменту у сфері захисту персональних даних. Проведено аналіз основних викликів, зокрема кіберзагроз, порушення конфіденційності, маніпулювання персональними даними та відсутності ефективного правового регулювання. Оцінено міжнародні підходи до етичного управління інформаційними ресурсами та корпоративну відповідальність за збереження конфіденційності. Стаття ґрунтується виключно на аналізі наукових робіт та нормативних документів, що регулюють питання кібербезпеки та інформаційної етики.

Ключові слова: *етика, інформаційний менеджмент, персональні дані, захист інформації, кібербезпека, корпоративна відповідальність, цифрова грамотність. етика, інформаційний менеджмент, персональні дані, захист даних, GDPR, корпоративна відповідальність, кібербезпека, цифрова грамотність.*

ETHICS IN INFORMATION MANAGEMENT: PERSONAL DATA PROTECTION

This article addresses the ethical dimensions of information management with a focus on personal data protection. Rapid digitalization has heightened the need for secure data handling and brought to light ethical dilemmas surrounding data privacy. The study identifies key challenges including cybersecurity threats, data breaches, and the ethical obligations of corporations to safeguard personal information in compliance with international regulations. Major international data protection standards (e.g., GDPR, ISO/IEC 27001) are evaluated, with particular attention to how corporate ethics foster transparency and accountability in data governance. The discussion underscores the importance of ethical guidelines for algorithmic decision-making—especially in AI systems—to mitigate issues such as algorithmic bias. Encryption technologies, advanced anonymization techniques, and blockchain solutions are highlighted as essential tools for ensuring data security and preventing unauthorized access. Case studies reveal that failures in data protection can lead to severe reputational and financial consequences, emphasizing the urgency for stronger regulatory enforcement. Beyond mere legal compliance, the article argues that corporate responsibility involves ethical leadership, robust security policies, and a culture of data privacy awareness. Collaboration among governments, businesses, and civil society is deemed vital for uniform global data protection standards. The article further explores how AI can both enhance and complicate data security, raising concerns about transparency and potential misuse of automated surveillance. Future research directions include examining the long-term effects of data protection regulations on innovation, the impact of digital literacy on security practices, and the implications of quantum computing for cryptography. The conclusion advocates a combined approach—integrating legal frameworks, technological advancements, and ethical responsibility—to protect personal data in an increasingly digital world.

Keywords*: ethics, information management, personal data, data protection, cybersecurity, corporate responsibility, digital literacy. ethics, information management, personal data, data protection, GDPR, corporate responsibility, cybersecurity, digital literacy.*

JEL classification*: M15, K24, L86.*

Постановка проблеми. У сучасному цифровому середовищі персональні дані стали стратегічним активом, що використовується у всіх сферах економіки, державного управління та соціальних відносин. Зростання обсягів оброблюваної інформації, розвиток хмарних технологій, штучного інтелекту та аналітики великих даних створює нові виклики щодо забезпечення конфіденційності, законності та етичності

використання персональних даних. У цьому контексті особливої актуальності набуває питання забезпечення інформаційної безпеки та правового захисту персональної інформації.

Однією з основних проблем є збільшення кількості випадків кіберзлочинності, що призводить до витоків конфіденційної інформації, фінансових втрат та репутаційних ризиків для компаній і державних установ. Недостатній рівень контролю за обробкою персональних даних, а також нерівномірність законодавчого регулювання у різних країнах створюють додаткові загрози для користувачів цифрових сервісів.

Ще одним критичним аспектом є використання персональних даних у комерційних цілях без належної згоди суб'єктів даних. Багато цифрових платформ та соціальних мереж збирають величезні масиви інформації про поведінку користувачів, що використовується для таргетованої реклами, політичного маніпулювання та соціальної інженерії. Це піднімає питання щодо меж законного використання персональної інформації та необхідності посилення механізмів контролю за діяльністю корпорацій у цій сфері.

Етичний аспект інформаційного менеджменту також є надзвичайно важливим. Недостатність корпоративної відповідальності, відсутність чітких внутрішніх політик щодо обробки персональних даних та недостатній рівень обізнаності персоналу щодо стандартів конфіденційності збільшують ризики порушення прав громадян. Організації повинні не лише дотримуватися чинних норм, а й розробляти власні етичні кодекси та політики управління інформацією, які забезпечать баланс між комерційними інтересами та правами користувачів.

Ще одним викликом є необхідність гармонізації національного законодавства з міжнародними стандартами. Регламент ЄС про захист персональних даних (GDPR) встановлює високі вимоги до безпеки та законності обробки даних, проте в багатьох країнах, включаючи Україну, нормативно-правова база ще потребує удосконалення. Важливим завданням є створення ефективних механізмів моніторингу та контролю за дотриманням цих стандартів на державному та корпоративному рівнях.

У зв'язку з цим постає необхідність розробки комплексного підходу до захисту персональних даних, який поєднує правові, технічні та етичні механізми регулювання. Важливо не лише посилювати державний контроль та відповідальність компаній, але й впроваджувати інноваційні технологічні рішення, такі як шифрування, блокчейн, багатофакторна автентифікація та машинне навчання для запобігання витокам інформації.

Таким чином, проблема захисту персональних даних є багатогранною і вимагає системного підходу до її вирішення. Вона включає питання правового регулювання, корпоративної етики, технологічної безпеки та цифрової грамотності. Це зумовлює необхідність проведення подальших досліджень у сфері інформаційної безпеки, а також розробки ефективних механізмів запобігання зловживанням у сфері управління персональними даними.

Аналіз останніх досліджень і публікацій. Дослідження у сфері захисту персональних даних активно ведуться в науковій спільноті, оскільки інформаційна безпека та кібернетика є критично важливими аспектами цифрового суспільства. Камінська Н.В. аналізує правові аспекти регулювання персональних даних, підкреслюючи необхідність гармонізації національного законодавства з міжнародними стандартами, зокрема GDPR [5]. У своїх дослідженнях вона звертає увагу на прогалини в законодавстві України, які ускладнюють реалізацію ефективного захисту персональних даних та створюють ризики для громадян у цифровому просторі.

Пилипчук В.Г. розглядає питання приватності та індивідуальних прав у контексті розвитку цифрових технологій та штучного інтелекту [3]. Автор підкреслює, що стрімке поширення алгоритмічного аналізу даних та автоматизованих систем ухвалення рішень значно впливає на персональну безпеку користувачів. Водночас, дослідження показують, що більшість сучасних підходів до обробки персональних даних не враховують етичні аспекти, що може призводити до дискримінації або порушення прав людини.

Осмятченко В.О., Згурська О.М. та Мартиненко М.О. акцентують увагу на ролі корпоративної етики у сфері ІТ, аналізуючи механізми впровадження відповідальних стандартів управління персональними даними [2]. Їхні дослідження показують, що дотримання етичних норм у великих корпораціях знижує ризики витоків інформації та сприяє формуванню довіри з боку користувачів. Вони також наголошують на необхідності розробки внутрішніх кодексів корпоративної поведінки, які визначатимуть відповідальність компаній за використання персональних даних.

Скибун О.Ж. аналізує етичні аспекти кібербезпеки, зосереджуючись на впливі цифрових технологій на інформаційну безпеку та захист прав користувачів [4]. Він наголошує на необхідності підвищення рівня цифрової грамотності населення, що є ключовим фактором у зниженні ризиків витоку персональних даних та кіберзлочинності. Автор також досліджує проблематику відповідальності державних органів та великих технологічних компаній за безпеку цифрової інфраструктури.

Брижко В.М. та Пилипчук В.Г. аналізують технологічні аспекти захисту персональних даних, зокрема роль шифрування, блокчейн-технологій та штучного інтелекту в забезпеченні інформаційної безпеки [6]. Дослідники підкреслюють, що ефективне впровадження таких технологій може суттєво знизити ризики несанкціонованого доступу до конфіденційної інформації та мінімізувати загрози від витоків даних.

Дуравкін П.М. та Гафич І.І. у своїх роботах досліджують майбутнє правового захисту персональних даних, аналізуючи вплив цифровізації на існуючі правові механізми [7]. Вони пропонують концепцію правової адаптації, яка передбачає гнучку систему нормативно-правових актів, що дозволяють ефективно реагувати на нові виклики у сфері інформаційної безпеки.

Попри значний обсяг наукових досліджень, все ще залишаються невирішені аспекти, зокрема питання ефективності реалізації міжнародних стандартів на національному рівні, правові наслідки використання штучного інтелекту для аналізу персональних даних та необхідність розробки загальносвітових механізмів контролю за обробкою інформації. Саме ці аспекти потребують подальшого вивчення та формування комплексних підходів до управління інформаційною безпекою.

Мета статті – аналіз сучасних підходів до етики інформаційного менеджменту, зокрема у контексті захисту персональних даних, а також розробка рекомендацій щодо вдосконалення механізмів регулювання інформаційної безпеки. У межах цього дослідження важливо розглянути ключові етичні проблеми, що виникають у процесі збирання, обробки та зберігання персональних даних, а також оцінити роль міжнародних та національних правових норм у створенні ефективної системи захисту конфіденційної інформації.

Дослідження також спрямоване на визначення впливу корпоративної відповідальності на управління персональними даними, зокрема на розгляд механізмів запровадження етичних стандартів в організаціях та компаніях, що працюють у цифровому секторі. Важливо оцінити, як компанії впроваджують внутрішні політики інформаційної безпеки та які практики можуть забезпечити підвищення рівня довіри серед користувачів.

Окремий аспект статті присвячено технологічним рішенням у сфері захисту персональних даних, серед яких розглядаються сучасні методи шифрування, технології блокчейн, автоматизовані системи кіберзахисту та штучний інтелект. Важливо оцінити ефективність їхнього впровадження, можливі обмеження та перспективи подальшого використання у сфері інформаційного менеджменту.

Крім того, стаття має на меті дослідити рівень цифрової грамотності серед користувачів, що є важливим фактором безпечного користування інформаційними ресурсами. Освітні ініціативи та державні програми цифрової грамотності можуть відіграти значну роль у зниженні ризиків витоків інформації та шахрайських дій у кіберпросторі. Саме тому важливо проаналізувати існуючі підходи до навчання громадян основам кібербезпеки та захисту персональних даних, а також запропонувати стратегії для їхнього вдосконалення.

Виклад основних результатів дослідження. Захист персональних даних є ключовим викликом сучасного інформаційного менеджменту. Швидкий розвиток технологій сприяє зростанню кіберзлочинності та витоків інформації, що потребує ефективного регулювання та відповідальних підходів до управління даними. Важливим аспектом залишається невідповідність національних правових норм міжнародним стандартам, що ускладнює процес захисту персональних даних у глобальному цифровому середовищі.

Сучасне законодавство, зокрема GDPR, встановлює суворі вимоги до обробки персональної інформації, зобов'язуючи організації дотримуватися принципів законності, прозорості та мінімізації даних. Водночас національні правові норми, такі як Закон України "Про захист персональних даних", лише частково відповідають європейським стандартам, що створює прогалини в ефективному контролі за дотриманням конфіденційності інформації.

Корпоративна етика є важливим фактором у забезпеченні інформаційної безпеки. Дотримання принципів відповідального зберігання та обробки даних сприяє формуванню довіри серед користувачів та партнерів компанії. Запровадження внутрішніх етичних кодексів, регулярний аудит систем безпеки та підвищення обізнаності працівників дозволяють мінімізувати ризики витоку інформації.

Технологічні рішення, такі як шифрування, блокчейн та штучний інтелект, є важливими інструментами для забезпечення конфіденційності даних. Інтеграція цих технологій у системи управління інформацією допомагає запобігти несанкціонованому доступу та втраті даних. Разом з тим їх ефективне використання вимагає розробки чітких регуляторних норм та стандартів впровадження.

Підвищення цифрової грамотності є невід'ємним компонентом ефективного захисту персональних даних. Освітні програми, орієнтовані на користувачів цифрових платформ, сприяють розумінню ризиків та підвищують рівень безпеки в цифровому середовищі.

Міжнародні стандарти захисту персональних даних мають суттєві відмінності, які впливають на ефективність регулювання у різних юрисдикціях, ключові відмінності між різними міжнародними підходами до захисту персональних даних. Порівняльний аналіз свідчить, що Україна потребує гармонізації законодавства відповідно до європейських стандартів для ефективного управління цифровими ризиками (табл 1).

Таблиця 1

Порівняльний аналіз міжнародних стандартів захисту персональних даних

Параметр	GDPR (ЄС)	Закон України "Про захист персональних даних"	ISO/IEC 27001
Законність обробки даних	Так	Так	Так
Принцип мінімізації даних	Так	Частково	Так
Право на забуття	Так	Ні	Ні
Штрафні санкції за порушення	Так	Обмежені	Ні
Контроль державного органу	Так	Так	Ні

Джерело: сформовано автором.

Висновок. Етика в інформаційному менеджменті, зокрема в аспекті захисту персональних даних, залишається критично важливою проблемою в умовах цифрової трансформації. Розвиток технологій, збільшення обсягів оброблюваної інформації та зростаюча кількість кіберзагроз вимагають комплексного підходу до захисту конфіденційності даних. Враховуючи сучасні виклики, поєднання правових, технологічних та організаційних механізмів забезпечення безпеки персональної інформації є пріоритетним напрямом для державних та приватних структур. Впровадження міжнародних стандартів, таких як GDPR та ISO/IEC 27001, сприяє підвищенню рівня безпеки персональних даних та адаптації до глобальних вимог цифрової епохи. Проте, національні правові системи, зокрема українське законодавство, потребують подальшого вдосконалення та гармонізації з європейськими нормами для створення ефективної регуляторної бази, що враховує специфіку локального цифрового ринку. Корпоративна відповідальність відіграє значну роль у забезпеченні інформаційної безпеки, оскільки організації повинні не лише дотримуватися правових вимог, але й активно впроваджувати політику етичного використання даних. Запровадження механізмів контролю, таких як внутрішній аудит безпеки, підвищення цифрової грамотності співробітників та розробка корпоративних стандартів етичного використання даних, може суттєво знизити ризики витоків інформації. Застосування сучасних технологічних рішень, включаючи шифрування, блокчейн та штучний інтелект, дозволяє суттєво зміцнити інформаційну безпеку. Водночас, їх ефективність напряму залежить від правильного впровадження та наявності законодавчих норм, які регулюють використання цих технологій у сфері персональних даних. Окрім цього, важливим залишається питання підвищення рівня цифрової грамотності серед користувачів, що дозволить уникати основних загроз, пов'язаних з обробкою персональної інформації. Державні та громадські ініціативи, спрямовані на навчання цифровій безпеці, повинні стати частиною стратегії забезпечення захисту персональних даних. Таким чином, етика в інформаційному менеджменті потребує комплексного підходу, що поєднує правові норми, корпоративну відповідальність та технологічні рішення. Подальші дослідження у цій сфері можуть бути спрямовані на аналіз впливу штучного інтелекту на обробку персональних даних, розробку ефективних механізмів захисту цифрової ідентичності та оцінку правових ризиків у сфері транснаціональної передачі персональних даних. Сучасні виклики інформаційного менеджменту потребують комплексного підходу, що поєднує правові, технологічні та етичні аспекти. Впровадження міжнародних стандартів, таких як GDPR, та розвиток корпоративної етики є необхідними для підвищення рівня захисту персональних даних. Перспективними напрямами досліджень є розробка нових механізмів управління інформаційними ризиками та впровадження інноваційних технологій безпеки.

Список використаних джерел:

1. Greene T. & Shmueli G. (2020). Beyond Our Behavior: The GDPR and Humanistic Personalized Recommendation. DOI: https://doi.org/10.48550/arXiv.2008.13404.
2. Осмятченко, В.О., Згурська, О.М., & Мартиненко, М.О. (2024). Вплив ділової етики на безпеку даних в IT- секторі в системі корпоративної культури. Проблеми сучасних трансформацій. Серія: економіка та управління, № 15. DOI: https://doi.org/10.54929/2786-5738-2024-15-04-03.
3. Пилипчук В.Г. (2017). Проблеми захисту приватності, індивідуальних свобод та безпеки людини в інформаційному суспільстві. Науковий часопис Національного педагогічного університету ім. М.П. Драгоманова. Серія 18: Право : зб. наук. праць. Київ : Вид-во НПУ ім. М.П. Драгоманова, Вип. 32. С. 106–119.
4. Скибун О.Ж. (2022). Сучасна етика як практична філософія кібербезпеки. Сучасний захист інформації, № 4. С. 66-70. DOI: https://doi.org/10.31673/2409-7292.2022.040011.
5. Камінська Н.В. (2015). Захист персональних даних: проблеми внутрішньодержавного, наднаціонального і міжнародно-правового регулювання. Науковий вісник Національної академії внутрішніх справ, № 3. С. 106-114. URL: https://elar.naiau.kiev.ua/bitstreams/e0d9506e-1d4b-4d6f-a952-6ed52d21ba5e/download.
6. Пилипчук В.Г., Брижко В.М. (2016). Інформаційна безпека та приватність у сфері захисту персональних даних. Інформація і право, № 4(19). С. 60-70. DOI: https://doi.org/10.37750/2616-6798.2016.4(19).272979.
7. Дуравкін, П., & Гафич, І. (2024). Сучасні виклики та майбутнє правового захисту персональних даних: під впливом розвитку цифровізації. Право та інновації, № 3(43). С. 89–100. DOI: https://doi.org/10.37772/2518-1718-2023-3(43)-12.
8. Предместніков О.Г., Посашева Д.В. (2023). Захист приватності та персональних даних у світі технологій. Правовий аспект. DOI: https://doi.org/10.36074/logos-26.05.2023.019.

References:

1. Greene T. & Shmueli G. (2020). Beyond Our Behavior: The GDPR and Humanistic Personalized Recommendation. DOI: https://doi.org/10.48550/arXiv.2008.13404. [in English].
2. Osmiatchenko, V.O., Zghurska, O.M., & Martynenko, M.O. (2024). Vplyv dilovoi etyky na bezpeku danykh v IT- sektori v systemi korporatyvnoi kultury [The impact of business ethics on data security in the IT sector in the corporate culture system]. Problems of modern transformations. Series: economics and management, No. 15.

DOI: https://doi.org/10.54929/2786-5738-2024-15-04-03. [in Ukranian].

3. Pylypchuk, V.G. (2017). Problemy zakhystu pryvatnosti, indyvidualnykh svobod ta bezpeky liudyny v informatsiinomu suspilstvi [Problems of protecting privacy, individual freedoms and human security in the information society]. Scientific journal of the National Pedagogical University named after M.P. Dragomanov. Series 18: Law: collection of scientific works. Kyiv: Publishing house of the National Pedagogical University named after M.P. Dragomanov, Iss. 32. Pp. 106–119. [in Ukranian].

4. Skybun, O.Zh. (2022). Suchasna etyka yak praktychna filosofiia kiberbezpeky [Modern ethics as a practical philosophy of cybersecurity]. Modern Information Protection, No. 4. Pp. 66-70. DOI: https://doi.org/10.31673/2409-7292.2022.040011. [in Ukranian].

5. Kaminska, N.V. (2015). Zakhyst personalnykh danykh: problemy vnutrishnoderzhavnoho, nadnatsionalnoho i mizhnarodno-pravovoho rehuliuvannia [Personal data protection: problems of domestic, supranational and international legal regulation]. Scientific Bulletin of the National Academy of Internal Affairs, No. 3. Pp. 106-114. Retrieved from: https://elar.naiau.kiev.ua/bitstreams/e0d9506e-1d4b-4d6f-a952-6ed52d21ba5e/download. [in Ukranian].

6. Pylypchuk, V.G., & Bryzhko, V.M. (2016). Informatsiina bezpeka ta pryvatnist u sferi zakhystu personalnykh danykh. [Information security and privacy in the field of personal data protection]. Information and Law, No. 4(19). Pp. 60-70. DOI: https://doi.org/10.37750/2616-6798.2016.4(19).272979. [in Ukranian].

7. Duravkin, P.M., & Hafych, I.I. (2024). Suchasni vyklyky ta maibutnie pravovoho zakhystu personalnykh danykh: pid vplyvom rozvytku tsyfrovizatsii [Modern challenges and the future of legal protection of personal data: influenced by the development of digitalization]. Law and Innovation, No. 3(43). Pp. 89–100. DOI: https://doi.org/10.37772/2518-1718-2023-3(43)-12. [in Ukranian].

8. Predmestnikov, O.G., & Posasheva, D.V. (2023). Zakhyst pryvatnosti ta personalnykh danykh u sviti tekhnolohii. Pravovyi aspect [Protection of privacy and personal data in the world of technology. Legal aspect]. DOI: https://doi.org/10.36074/logos-26.05.2023.019.