УДК 342.7:342.9:340.5
DOI https://doi.org/10.32999/ksu2307-8049/2026-4-14

ПРАВОВИЙ СТАТУС ОРГАНІВ, ЯКІ ЗАЙМАЮТЬСЯ ЗАХИСТОМ ПЕРСОНАЛЬНИХ ДАНИХ, ПОРІВНЯЛЬНО-ПРАВОВЕ ДОСЛІДЖЕННЯ

Рябченко Максим Олександрович,
аспірант спеціальності «Право»
Сумського державного університету
ryaba200058@gmail.com
https://orcid.org/0009-0003-0317-9536K

Метою статті є *комплексне дослідження правового статусу органів, уповноважених здійснювати нагляд і контроль у сфері захисту персональних даних в Україні та зарубіжних державах, актуальність якого зумовлена стрімким розвитком цифрових технологій та євроінтеграційними зобов'язаннями щодо гармонізації національного законодавства із правом Європейського Союзу.*

Методи. *На основі порівняльно-правового аналізу досліджено досвід функціонування органів захисту персональних даних у Німеччині, Франції та Польщі, охарактеризовано їхню організаційну структуру, компетенцію, контрольні повноваження та механізми застосування заходів впливу. Для з'ясування правового статусу досліджуваних органів застосовано формально-юридичний метод.*

Результати. *Проаналізовано сучасну модель державного контролю у сфері захисту персональних даних в Україні, визначено її переваги, недоліки та проблемні аспекти функціонування в умовах цифрової трансформації державного управління. Особливу увагу приділено міжнародно-правовим стандартам організації діяльності незалежних наглядових органів, закріпленим у Загальному регламенті Європейського Союзу про захист даних (GDPR), а також принципам їх інституційної незалежності, ефективності та функціональної автономії. Виокремлено децентралізовану модель Федерального уповноваженого із захисту даних Німеччини, колегіальну модель Національної комісії з питань інформатики та свободи Франції та управлінську модель Управління захисту персональних даних Польщі. Визначено основні відмінності між українською моделлю державного контролю та європейськими підходами до забезпечення ефективного нагляду за дотриманням законодавства у сфері захисту персональних даних.*

Висновки. *Обґрунтовано необхідність подальшого вдосконалення національної системи захисту персональних даних шляхом створення інституційно незалежного спеціалізованого органу державного контролю, розширення його повноважень, посилення організаційної та фінансової автономії, а також імплементації найкращих європейських практик у національне законодавство. Аргументовано доцільність ліквідації моделі контролю, покладеної на Уповноваженого Верховної Ради України з прав людини, та утворення Національної комісії з питань захисту персональних даних, наділеної правом самостійного накладення штрафів, повноваженнями у сфері кіберзахисту в умовах воєнного стану, а також функціями впровадження обов'язкової Оцінки впливу на захист даних (DPIA).*

Ключові слова: *персональні дані, захист персональних даних, правовий статус, наглядовий орган, GDPR, право на приватність, інформаційне право, євроінтеграція.*

LEGAL STATUS OF PERSONAL DATA PROTECTION AUTHORITIES: A COMPARATIVE LEGAL STUDY

Riabchenko Maksym Oleksandrovych,
Postgraduate Student in Law
Sumy State University
ryaba200058@gmail.com
https://orcid.org/0009-0003-0317-9536

The purpose *of the article is a comprehensive study of the legal status of authorities empowered to exercise supervision and control in the field of personal data protection in Ukraine and foreign countries, the relevance of which is driven by the rapid development of digital technologies and European integration obligations regarding the harmonization of national legislation with European Union law.*

Methods. *On the basis of a comparative legal analysis, the experience of personal data protection authorities' functioning in Germany, France, and Poland has been examined, and their organizational structure, competence, control powers, and mechanisms for applying enforcement measures have been characterized. To clarify the legal status of the studied authorities, the formal-legal method was applied.*

Results. *The current model of state control in the field of personal data protection in Ukraine has been analyzed, and its advantages, shortcomings, and problematic aspects of functioning under the conditions of digital transformation of public administration have been identified. Particular attention has been paid to international legal standards governing the organization of independent supervisory authorities' activities,*

© Рябченко М. О., 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

as enshrined in the General Data Protection Regulation of the European Union (GDPR), as well as to the principles of their institutional independence, effectiveness, and functional autonomy. Three models have been distinguished: the decentralized model of the Federal Commissioner for Data Protection and Freedom of Information in Germany, the collegial model of the National Commission for Informatics and Liberties in France, and the managerial model of the Personal Data Protection Office in Poland. The main differences between the Ukrainian model of state control and European approaches to ensuring effective supervision of compliance with personal data protection legislation have been identified.

Conclusions. *The necessity of further improving the national system of personal data protection has been substantiated through the establishment of an institutionally independent specialized state control authority, the expansion of its powers, the strengthening of its organizational and financial autonomy, and the implementation of best European practices into national legislation. The expediency has been argued of liquidating the control model currently vested in the Ukrainian Parliament Commissioner for Human Rights and establishing a National Commission for Personal Data Protection, empowered to impose fines directly, to exercise powers in the field of cyber defense under martial law, and to perform functions related to the implementation of a mandatory Data Protection Impact Assessment (DPIA).*

Keywords: *personal data, personal data protection, supervisory authority, legal status, GDPR, right to privacy, information law, European integration.*

Вступ. Стрімкий розвиток інформаційного суспільства, цифровізація публічного управління та активне впровадження сучасних інформаційно-комунікаційних технологій істотно впливають на зміст і механізми реалізації основоположних прав людини. Одним із найбільш чутливих аспектів цифрової трансформації суспільних відносин є забезпечення права особи на охорону приватних відомостей. Варто зауважити, що фундаментальним нормативним базисом для унормування цих відносин виступає Конституція України, стаття 32 якої імперативно забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди (Конституція України, 1996). Водночас розширення сфер використання персональних даних супроводжується підвищенням ризиків їх незаконного збирання, обробки, поширення та використання, що зумовлює необхідність удосконалення правових та інституційних механізмів їх убезпечення.

Однією з ключових передумов цифрової інтеграції відповідно до міжнародних стандартів є забезпечення належного рівня захисту персональних даних відповідно до вимог європейських стандартів. Як свідчить історіографія дослідження інтеграції законодавства України до правових стандартів ЄС (Гамалій, 2026), цей процес потребує концептуальної гармонізації інституційних інструментів контролю. Важливе значення у цьому процесі має імплементація положень Регламенту (ЄС) 2016/679 (General Data Protection Regulation – GDPR) (GDPR, 2016), який встановлює високі стандарти охорони індивідуальних даних та передбачає функціонування незалежних наглядових органів, уповноважених здійснювати контроль за дотриманням законодавства у відповідній сфері. Водночас чинна модель державного контролю у сфері захисту персональних даних в Україні залишається предметом наукових дискусій щодо її ефективності, інституційної спроможності та відповідності сучасним європейським стандартам.

Проблематика охорони персональних даних та функціонування механізмів державного контролю у зазначеній сфері неодноразово ставала предметом наукових досліджень. Організаційно-правові аспекти захисту персональних даних досліджувалися у працях М. М. Бліхар (Бліхар, 2023), яка розглядала механізми забезпечення права на убезпечення конфіденційної інформації та особливості їх правового регулювання. Питання адміністративно-правового забезпечення відносин щодо обробки персональних даних знайшли відображення у роботах М. В. Різака (Різак, 2018). Особливості правового регулювання використання персональних даних стали предметом дослідження Ю. В. Осики (Осика, 2023). Окремі аспекти забезпечення захисту персональних даних у сучасних умовах цифрової трансформації розкривалися у працях А. С. Михайлика (Михайлик, 2021).

Значний науковий інтерес становлять дослідження О. В. Різенка, присвячені загальним правовим стандартам у сфері захисту персональних даних (Різенко, 2024), та Р. А. Пристая – безпосередньому аналізу ролі та практики діяльності національних органів захисту даних у державах Європейського Союзу, зокрема в соціальних мережах (Пристай, 2024). Важливе значення для формування теоретичної основи дослідження мають положення GDPR (GDPR, 2016), сучасні орієнтири антикорупційної політики держави (Лисак, 2026), а також аналітичні матеріали Міністерства цифрової трансформації щодо адаптації українського законодавства до права Європейського Союзу у сфері відкритих даних (Роїк, 2023).

Поряд із цим, попри наявність значної кількості наукових праць, недостатньо дослідженими залишаються питання правового статусу органів, уповноважених здійснювати державний контроль у сфері захисту персональних даних, особливо в контексті сучасних євроінтеграційних процесів та цифрової трансформації державного управління. Подальшого наукового осмислення потребують також проблеми забезпечення інституційної незалежності таких органів, визначення оптимального обсягу їхніх повноважень, а також адаптації національної моделі державного контролю до вимог GDPR та практики держав-членів

Європейського Союзу. Крізь призму аналізу функціонування делегованого законодавства в Україні та євроінтеграційних бенчмарків (Катилов, 2026), підтверджується необхідність дотримання суворих правових стандартів незалежного публічного контролю.

Наукова новизна полягає у комплексному порівняльно-правовому аналізі моделей державного контролю у сфері захисту персональних даних та обґрунтуванні доцільності запровадження в Україні незалежного колегіального органу з правом самостійного накладення штрафів, повноваженнями кіберзахисту в умовах воєнного стану та впровадження обов'язкової DPIA.

Мета статті полягає у комплексному дослідженні правового статусу органів, уповноважених на захист персональних даних в Україні та зарубіжних державах, здійсненні порівняльно-правового аналізу відповідних інституційних моделей та розробленні пропозицій щодо вдосконалення національної системи державного контролю у сфері захисту персональних даних.

Для досягнення поставленої мети пропонується розв'язати такі завдання: дослідити правові засади функціонування органів захисту персональних даних в Україні; проаналізувати міжнародні та європейські стандарти діяльності наглядових органів у відповідній сфері; здійснити порівняльно-правову характеристику органів захисту персональних даних у державах Європейського Союзу; визначити основні проблеми функціонування чинної моделі державного контролю в Україні; сформулювати пропозиції щодо вдосконалення правового статусу органів захисту персональних даних з урахуванням європейського досвіду.

Методологічну основу дослідження становлять порівняльно-правовий метод (зіставлення моделей державного контролю в Україні, Німеччині, Франції та Польщі), формально-юридичний метод (аналіз норм національного законодавства та GDPR) і системно-структурний метод (аналіз організаційної побудови та повноважень досліджуваних органів).

Логіка представлення матеріалу зумовлена завданнями дослідження: послідовно розглянуто сучасний стан державного контролю в Україні, європейські стандарти GDPR, зарубіжний досвід Німеччини, Франції та Польщі, а також пропозиції щодо вдосконалення національної моделі.

1. Становлення механізму захисту даних в Україні

Первинний організаційно-правовий каркас захисту приватності в Україні створювався у повній відповідності до міжнародних орієнтирів кінця XX століття. Основоположним вітчизняним документом у відповідній сфері правовідносин став Закон України від 01.06.2010 № 2297-VI «Про захист персональних даних», спрямований на імплементацію Конвенції Ради Європи № 108 та положень тогочасної Директиви 95/46/ЄС.

Для забезпечення державного контролю у сфері захисту персональних даних у 2011 році було утворено Державну службу України з питань захисту персональних даних як центральний орган виконавчої влади зі спеціальним статусом. Її створення стало одним із перших інституційних кроків щодо реалізації положень Закону України від 01.06.2010 № 2297-VI «Про захист персональних даних» та виконання міжнародних зобов'язань України у відповідній сфері. (Пристай, 2024: 246). Профільне відомство мало забезпечити чітку координацію між реєстрами та мінімізувати ризики несанкціонованого доступу до приватних відомостей громадян, закладаючи фундамент національної безпеки у кіберпросторі.

Проте у 2014 році, в межах масштабного скорочення та оптимізації державного апарату, зазначену Службу було ліквідовано, а її повноваження у повному обсязі передано Уповноваженому Верховної Ради України з прав людини (Пристай, 2024: 246). З цього моменту в Україні закріпилася унікальна, але вкрай суперечлива модель наглядової діяльності. Варто зауважити, що охорона персональних даних через це фактично перетворилася на один із багатьох напрямів роботи інституту Омбудсмана, що суттєво розмило спеціалізацію державного нагляду.

2. Проблеми чинної моделі державного контролю

Відповідно до ст. 22 профільного нормативно-правового акту на Омбудсмана покладаються функції з розгляду скарг, проведення планових і позапланових, виїзних та безвиїзних перевірок володільців чи розпорядників даних, доступу до будь-якої конфіденційної інформації та видачі обов'язкових для виконання приписів про усунення правопорушень (Про захист персональних даних, 2010).

На реалізацію цих норм Секретаріат Уповноваженого розробив відповідні акти, якими унормовано типовий порядок обробки персональних даних та процедуру здійснення перевірок (Пристай, 2024: 247). Цей нормативний масив мав врегулювати порядок взаємодії державних інституцій та приватних суб'єктів, проте на практиці процедури виявилися занадто бюрократизованими.

Попри тривале функціонування цієї моделі, сучасний стан суспільних відносин виявив системну недостатність її організаційної та кадрової спроможності, що не відповідає міжнародним стандартам незалежного нагляду: за офіційною відповіддю Секретаріату Уповноваженого на інформаційний запит, підрозділ із захисту персональних даних станом на 2018 рік налічував лише 13 співробітників з бюджетом до 150 тис. євро, тоді як британський орган нагляду того ж року – 700 осіб (Korchynskyi et al., 2020).

По-перше, інститут Омбудсмана за своєю правовою природою є парламентським органом правозахисного, парламентського контролю, мета якого – захист індивіда від зловживань з боку державного апарату. Покладення

на нього функцій класичного адміністративного регулятора, який повинен контролювати не лише державні органи, а й колосальний масив суб'єктів приватного бізнесу (банки, страхові компанії, IT-сектор, ритейл), створює глибоку концептуальну колізію та перевантажує Секретаріат непритаманними для нього функціями (Пристай, 2024: 246).

По-друге, чинний правовий інструментарій Омбудсмана є пасивним та процедурно відірваним від реальності: за наявності серйозних правопорушень він здатний лише складати протоколи про адміністративні правопорушення, що в умовах завантаженості судової системи здебільшого призводить до закриття справ за строками давності та нівелює принцип невідворотності покарання (Пристай, 2024: 251). Брак механізмів прямого впливу робить державний нагляд декларативним.

По-третє, Закон України від 01.06.2010 № 2297-VI «Про захист персональних даних» (Про захист персональних даних, 2010) безнадійно застарів, оскільки поза увагою законодавцем були залишені відносини спільної обробки даних у мережі Інтернет, транскордонні потоки інформації в епоху хмарних технологій та особливості функціонування масштабних публічних реєстрів (Костюк та ін., 2025; Роїк, 2023). Нормативний вакуум не дозволяє ефективно протидіяти новітнім цифровим загрозам. Поза увагою законодавця залишилися й питання належного правового регулювання обробки біометричних персональних даних, зростаюче використання яких у правоохоронній та профілактичній діяльності потребує посиленого правового захисту (Стратонов, Савєльєва, 2020; Konovalova et al., 2021).

Нинішня національна модель контролю, на наше переконання, не відповідає критеріям повної «інституційної та фінансової незалежності», оскільки Омбудсман фінансується за загальною статтею забезпечення Верховної Ради і не має автономних ресурсів для розбудови потужного матеріально-технічного та експертного підґрунтя, що прямо гальмує виконання Україною зобов'язань щодо гармонізації законодавства (Пристай, 2024: 246). Без фінансової автономії принципово неможливо створити сучасні інструменти захищеності персональних даних.

3. Європейські стандарти незалежного нагляду

Для побудови ефективного регулятора в Україні критично важливим є глибоке осмислення європейського досвіду, де право на приватність піднесено до рівня фундаментального права первинного законодавства. Основним актом у цій сфері виступає Регламент ЄС 2016/679 (GDPR), який уніфікував правила обробки даних на всьому просторі співтовариства з метою забезпечення високого рівня приватності та вільного руху інформації на внутрішньому ринку.

Стаття 51 GDPR (GDPR, 2016) чітко зобов'язує кожну державу-члена утворити один або кілька незалежних публічних наглядових органів (Data Protection Authorities – DPA). Наднаціональним координаційним центром виступає Європейська рада із захисту персональних даних (ЄРЗПД), заснована відповідно до ст. 68 GDPR, яка складається з керівників усіх національних DPA та Європейського інспектора із захисту даних. Головна мета ЄРЗПД – забезпечення послідовного та однолінійного застосування правил щодо захисту приватності у всьому Євросоюзі (Різенко, 2024а: 646). Цей інституційний контур гарантує, що безпека особистої інформації одноманітно забезпечується на всьому європейському континенті, незалежно від юрисдикції конкретної країни.

4. Досвід Німеччини, Франції та Польщі

Аналіз правового статусу DPA у провідних країнах Європи дозволяє виділити кілька успішних моделей організації. До прикладу, у Німеччині діє інститут Федерального уповноваженого із захисту даних і свободи інформації (BfDI). Відповідно до § 8 Федерального закону про захист даних (BDSG), BfDI є «незалежним федеральним органом вищого рівня» (oberste Bundesbehörde), а § 10 BDSG гарантує його повну незалежність, зазначаючи, що Уповноважений при виконанні своїх обов'язків «підпорядковується тільки закону та не підлягає жодному правовому чи службовому нагляду» (BDSG, 2017). Німецька модель цікава своєю децентралізацією, де федеральний устрій накладає відбиток на функціонування земельних наглядових відомств.

Натомість у Франції наглядові функції покладено на Національну комісію з питань інформатики та свобод (CNIL). Згідно зі ст. 8 Закону Франції № 78-17 від 6 січня 1978 р. «Про інформатику, файли та свободи», CNIL визначено як «незалежний адміністративний орган», який діяльно «забезпечує відповідність обробки персональних даних положенням цього Закону та Регламенту (ЄС) 2016/679» (Loi n° 78-17, 1978). Законодавець прямо закріплює за колегією CNIL роль гаранта захисту фундаментальних прав і свобод людини у цифровому середовищі.

У Республіці Польща функціонує Управління захисту персональних даних (UODO) на чолі з Президентом Управління. Відповідно до ст. 34 Закону Польщі від 10 травня 2018 р. «Про захист персональних даних», Президент UODO є «орган, уповноважений здійснювати нагляд за дотриманням положень про захист персональних даних», який під час виконання своїх завдань «є незалежним та підпорядковується лише закону» (Ustawa, 2018).

За єдиними критеріями розглянуті моделі відрізняються насамперед порядком утворення та ухвалення рішень: Федеральний уповноважений Німеччини обирається Бундестагом на п'ять років (BDSG, 2017), Президент UODO призначається Сеймом за згодою Сенату на чотири роки (Ustawa, 2018), і обидва діють одноосібно, тоді як CNIL є колегіальним органом із 18 членів, а санкції накладає його окрема «обмежена формація» (Loi n° 78-17, 1978). Спільними для всіх трьох

ISSN: 2307-8049 (Print)
ISSN: 2663-2799 (Online)

є підпорядкованість лише закону, окремий рядок державного бюджету, право накладати штрафи до 20 млн євро або 4% світового обороту (GDPR, 2016) та оскарження рішень в адміністративних судах.

Польський досвід є найбільш релевантним для України, оскільки демонструє швидку трансформацію пострадянської системи контролю у сучасний та дієвий інструмент забезпечення приватності користувачів. Громадяни цих держав мають змогу звернутися до DPA у режимі реального часу через зручні електронні форми, відстежуючи стан розгляду заяв онлайн (Пристай, 2024: 247).

5. Санкційні повноваження та практика ЄС

Ключовою рисою, що кардинально відрізняє європейські DPA від українського Омбудсмана, є наявність потужних імперативних, розслідувальних та каральних повноважень, визначених ст. 58 GDPR (GDPR, 2016). У 2023 році Європейська рада з захисту даних уніфікувала розрахунок штрафів за порушення GDPR, затвердивши єдину п'ятиетапну методологію, обов'язкову для застосування всіма національними наглядовими органами (EDPB, 2023).

Зокрема, європейські регулятори мають достатній інструментарій для здійснення глибоких технічних аудитів, мають безперешкодний доступ до серверів, видають обов'язкові приписи, повністю зупиняють транскордонні потоки даних у разі виявлення загроз безпеці, а головне – наділені правом самостійно накладати великі адміністративні штрафи. Завдяки цьому забезпечується невідворотність відповідальності за будь-які маніпуляції з конфіденційними масивами відомостей.

Ефективність такого підходу підтверджується офіційною статистикою: за порушення GDPR європейськими органами стягнули сотні мільйонів євро, що змусило глобальний бізнес повністю переглянути свою корпоративну політику приватності (Різенко, 2024: 647). Найбільш показовим є кейс Ірландської комісії із захисту даних (DPC), яка наклала безпрецедентний штраф у розмірі 1,2 млрд євро на корпорацію Meta Platforms за незаконну передачу даних європейських користувачів до США із порушенням ст. 44 GDPR (GDPR Enforcement Tracker, 2023).

Цей прецедент довів, що навіть найбільші транснаціональні корпорації змушені рахуватися з національними регуляторами. Іншим прикладом є штраф у розмірі 50 тис. євро, накладений Бельгійським DPA на соціальну мережу за незаконне використання функції «запроси друга» та збирання даних осіб без їх дійсної згоди (APD/GBA, 2020). Ще одним показовим прикладом є рішення CNIL від 1 вересня 2025 року про накладення штрафу в розмірі 325 млн євро на корпорацію Google за порушення правил використання рекламних та cookie-технологій у сервісі Gmail (CNIL, 2025).

Важливим елементом європейської моделі є також транскордонна кооперація та спільні розслідування (joint investigation) в межах механізму «єдиного вікна» (One-Stop-Shop), коли рішення DPA однієї країни, де розташована штаб-квартира компанії, автоматично змінює практику захисту прав громадян в усіх інших державах-членах ЄС (Пристай, 2024: 248).

Крім того, європейські DPA виступають проактивними інституціями: вони заохочують створення галузевих Кодексів поведінки (Code of Conduct), розробляють суворі вимоги до Оцінки впливу на захист даних (DPIA) для профілювання та штучного інтелекту, а також ведуть відкритий облік усіх застосованих санкцій, що забезпечує найвищий рівень прозорості та правової визначеності. У такий спосіб формується передбачуване та безпечне цифрове середовище для бізнесу та соціуму.

6. Пропозиції щодо реформування регулятора

Спираючись на критичний аналіз міжнародних стандартів та враховуючи специфіку сучасного українського правового середовища, автор пропонує власну концепцію реформування правового статусу наглядового органу в Україні. Очевидно, що подальше зволікання із інституційною модернізацією не лише поглиблює кризу приватності всередині держави, а й створює прямі перепони для виходу вітчизняного бізнесу на міжнародні ринки та блокує повноцінне інтеграційне входження України до Єдиного цифрового ринку ЄС. Наші підприємства опиняються у дискримінаційному становищі через невідповідність національних стандартів європейським вимогам «адекватності» (adequacy decision).

Першою і ключовою авторською пропозицією є виведення функцій нагляду у сфері захисту персональних даних з компетенції Уповноваженого ВРУ з прав людини. Натомість необхідно утворити принципово новий державний орган зі спеціальним статусом – Національну комісію з питань захисту персональних даних. Даний орган має бути побудований за колегіальним принципом, фінансуватися за окремим захищеним рядком Державного бюджету та мати повну інституційну автономію від політичних впливів. Колегіальність прийняття рішень дозволить уникнути суб'єктивізму та забезпечить всебічний розгляд складних кейсів у сфері IT-індустрії.

Другою важливою ідеєю є радикальна зміна характеру повноважень майбутнього регулятора: його рішення повинні мати імперативний, а не лише рекомендаційний характер, а самому Органу має бути надано право прямого, позасудового накладення адміністративно-фінансових штрафів на суб'єктів господарювання та органи влади за прикладом європейських DPA (Пристай, 2024: 250). Однак позасудовий порядок накладення штрафів не має позбавляти суб'єкта господарювання процесуальних гарантій. За зразком ст. 78 GDPR, необхідно надати можливість оскаржувати рішення Нацкомісії повинно оскаржуватися до адмінсуду з автоматичним зупиненням його виконання до набранням рішення законної

сили. Це дозволить подолати хронічну неефективність вітчизняних адміністративних процедур та змусить розпорядників інформації відповідально ставитися до убезпечення конфіденційної інформації громадян.

Третьою, сутнісною новелою авторської концепції є адаптація функцій наглядового органу до екстремальних воєнних викликів сьогодення (Катилов, 2026: 29). Досвід ведення гібридної війни довів, що персональні дані громадян перетворилися на зброю в руках агресора, який створює фішингові платформи для збору відомостей про родини військовослужбовців ЗСУ та організації фільтраційних заходів на тимчасово окупованих територіях.

Спираючись на концептуальні пропозиції В. І. Катилова щодо необхідності посилення публічно-правового захисту реєстрів та збалансування швидкості прийняття актів уряду із суворим наглядом (Катилов, 2026: 29), наголошуємо на необхідності створення у структурі нової Національної комісії спеціалізованих підрозділів із гібридними повноваженнями.

Ці підрозділи мають поєднувати класичний правовий нагляд із заходами активного кіберзахисту, здійснювати постійний проактивний моніторинг інцидентів безпеки державних баз даних та взаємодіяти з органами кіберполіції та СБУ для оперативного блокування ворожих ресурсів (Пристай, 2024: 250). Актуальність цієї функції підтверджує кібератака на реєстри Міністерства юстиції України 19 грудня 2024 року, яка паралізувала державні реєстри персональних даних на понад місяць, тоді як орган захисту персональних даних не мав самостійних повноважень ні оцінити наслідки для суб'єктів даних, ні вимагати від розпорядника повідомлення про витік (Економічна правда, 2024). В умовах збройного конфлікту охорона приватних даних перестає бути виключно питанням права особи, а стає важливою складовою національної безпекової політики Держави.

Четвертою пропозицією є нормативне закріплення проактивних європейських інструментів: новий орган має розробити та впровадити обов'язкові національні стандарти проведення Оцінки впливу на захист даних (DPIA) під час розгортання нових інформаційних систем у сфері медицини (eHealth), соціального забезпечення та електронного урядування, а також активно стимулювати розробку галузевих Кодексів поведінки для приватного бізнесу (Пристай, 2024: 246, 248). Це дозволить створити превентивну систему захищеності інформації, де ризики витоку відомостей прораховуються ще на етапі проєктування будь-якого цифрового сервісу.

Висновки. Проведене порівняльно-правове дослідження дозволило встановити, що чинна модель державного контролю у сфері захисту персональних даних в Україні лише частково відповідає європейським стандартам, оскільки передача повноважень Омбудсману не створила передумов для формування інституційно незалежного наглядового органу. Водночас досвід ЄС засвідчує, що ефективна безпека особистої інформації пов'язана з функціонуванням автономних інституцій, наділених широкими санкційними повноваженнями.

Імплементація вимог GDPR вимагає створення в Україні спеціалізованого незалежного регулятора з належним рівнем фінансової та функціональної автономії. Такі кроки підвищать ефективність нагляду, посилять захищеність особи в цифровому середовищі та забезпечать гармонізацію вітчизняного законодавства з європейським правом. Перспективи подальших наукових пошуків полягають у вивченні взаємодії майбутнього органу з відомствами кібербезпеки та адаптації української системи гарантування цифрової приватності до новітніх актів ЄС.

Декларація про використання штучного інтелекту. Автор використовував інструмент штучного інтелекту «Claude 3.5 Sonnet» виключно з метою виправлення граматичних і стилістичних помилок, а також для уніфікації та форматування списку літератури. Інструменти ШІ не застосовувалися для генерування наукових ідей, змісту роботи чи висновків.

Конфлікт інтересів. Автор заявляє про відсутність конфлікту інтересів.

ЛІТЕРАТУРА:

1. Бліхар М. М. Організаційно-правовий механізм захисту персональних даних. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Вип. 77, ч. 2. С. 31–36. DOI https://doi.org/10.24144/2307-3322.2023.77.2.4

2. Гамалій І. В. Історіографія дослідження інтеграції законодавства України до правових стандартів ЄС. *Прикарпатський юридичний вісник.* 2026. Випуск 1 (66). С. 12–17. DOI https://doi.org/10.32782/pyuv.v1.2026.3

3. Пропало все: як російські хакери зламали українські реєстри. Економічна правда. 20.12.2024. URL: https://epravda.com.ua/tehnologiji/propalo-vse-yak-rosiyski-hakeri-zlamali-ukrajinski-reyestri-801172/.

4. Катилов В. І. Делеговане законодавство в Україні крізь призму євроінтеграційних бенчмарків та стандартів International IDEA. *Прикарпатський юридичний вісник.* 2026. Випуск 1 (66). С. 29–34. DOI https://doi.org/10.32782/pyuv.v1.2026.6

5. Конституція України : Закон від 28 черв. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

6. Костюк Ю. В., Складанний П. М., Гулак Г. М., Бебешко Б. Т., Хорольська К. В., Рзаєва С. Л. Системи захисту інформації : підручник. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 887 с. URL: https://elibrary.kubg.edu.ua/id/eprint/51359/1/Kostiuk_Y_Skladannyi_P_Hulak_H_Bebeshko_B_Khorolska_K_Rzaieva_S_SZI_2025_FITM.pdf.

7. Лисак С.-Ю. Ю. Антикорупційна політика сучасної держави: європейські орієнтири та напрямки розвитку. *Прикарпатський юридичний вісник.* 2026. Випуск 1 (66). С. 35–38. DOI https://doi.org/10.32782/pyuv.v1.2026.7

8. Михайлик А. С. Сучасний стан та проблеми захисту персональних даних працівників в Україні в умовах цифрової трансформації. *Соціальне право.* 2021. № 4. С. 200–207. URL: https://ir.library.knu.ua/handle/15071834/24866

9. Осика Ю. В. Правове регулювання використання персональних даних. *Ірпінський юридичний часопис.* 2023. Вип. 3 (12). С. 343–351. DOI 10.33244/2617-4154.3(12).2023.343-351

10. Різенко О. В. Європейські правові стандарти захисту персональних даних. Аналітично-порівняльне правознавство.

2024. № 6. С. 643–648. DOI: https://doi.org/10.24144/2788-6018.2024.06.105

11. Пристай Р. А. Національні органи захисту даних в Європейському Союзі: роль і практика в сфері захисту персональних даних в соціальних мережах. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 82, ч. 2. С. 245–252. DOI https://doi.org/10.24144/2307-3322.2024.82.2.39

12. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України.* 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

13. Різак М. В. Адміністративно-правове забезпечення відносин обігу та обробки персональних даних в Україні : автореф. дис. ... д-ра юрид. наук : 12.00.07 / Харківський національний університет внутрішніх справ. Харків, 2018. 39 с. URL: https://dspace.univd.edu.ua/items/b86b4c7d-d0b7-460f-9c06-fd5095416024.

14. Роїк М. Відповідність законодавства України окремим положенням правового регулювання сфери відкритих даних у Європейському Союзі : Аналітичний Звіт / за ред. О. Заярного. Київ : Міністерство цифрової трансформації України, 2023. 31 с. URL: https://eef.org.ua/wp-content/uploads/2023/07/Vidpovidnist-zakonodavstva-Ukrayiny-okremym-polozhennyam-pravovogo-regulyuvannya-sfery-vidkrytyh-danyh-u-YEvropejskomu-Soyuzi.pdf.

15. APD/GBA. Beslissing ten gronde / Décision quant au fond n° 25/2020 du 14 mai 2020. Autorité de protection des données. URL: https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/Beslissing_GK_25-2020_EN.pdf

16. Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 1 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist. URL: https://www.gesetze-im-internet.de/bdsg_2018/

17. CNIL. Publicités insérées entre les courriels et cookies : la CNIL sanctionne GOOGLE d'une amende de 325 millions d'euros. Paris : Commission Nationale de l'Informatique et des Libertés, 03.09.2025. URL: https://www.cnil.fr/fr/thematique/cnil/sanctions.

18. European Data Protection Board. Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 2.1. Brussels : EDPB, 2023.

19. General Data Protection Regulation (GDPR) : Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union.* 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504.

20. GDPR Enforcement Tracker : Report / CMS Law. 2023. Fine ID: ET-2212 (TikTok Technology Limited). URL: https://www.enforcementtracker.com/

21. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

22. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dz.U. 2018 poz. 1000. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000

23. Korchynskyi D., Kobrin A., Nekrutenko V. Ukrainian GDPR: The reality and future of privacy legislation in Ukraine. IAPP, 28.09.2020. URL: https://iapp.org/news/a/ukrainian-gdpr-the-reality-and-future-of-privacy-legislation-in-ukraine.

24. Стратонов В. М., Савєльєва І. В. Окремі аспекти використання біометричних персональних даних у профілактиці правопорушень. Юридичний бюлетень. 2020. Вип. 16. С. 265–271. DOI https://doi.org/10.32850/LB2414-4207.2020.16.35

25. Stratonov V., Konovalova V., Savelieva I. Biometric personal data and their use in the investigation of criminal offences. Journal of the National Academy of Legal Sciences of Ukraine. 2021. Vol. 28, No. 4. DOI https://doi.org/10.24144/2307-3322.2024.82.2.39

REFERENCES:

1. Blikhar M. M. (2023). Organizatsijno-pravovyi mekhanizm zakhystu personalnykh danykh [Organizational and Legal Mechanism for Personal Data Protection]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Scientific Bulletin of Uzhhorod National University. Series: Law. Issue 77 (2). P. 31–36. DOI https://doi.org/10.24144/2307-3322.2023.77.2.42.

2. Hamalii I. V. (2026). Istoriohrafiia doslidzhennia intehratsii zakonodavstva Ukrainy do pravovykh standartiv YES [Historiography of Research on the Integration of Ukrainian Legislation into EU Legal Standards]. Prykarpatskyi iurydychnyi visnyk – Subcarpathian Law Bulletin. Issue 1 (66). P. 12–17. DOI https://doi.org/10.32782/pyuv.v1.2026.3

3. Propalo vse: yak rosiiski khakeri zlamaly ukrainski reyestry [All is Lost: How Russian Hackers Hacked Ukrainian Registers]. Ekonomichna pravda – Economic Truth. December 20, 2024. URL: https://epravda.com.ua/tehnologiji/propalo-vse-yak-rosiyski-hakeri-zlamali-ukrajinski-reyestri-801172/.

4. Katylov V. I. (2026). Delehovane zakonodavstvo v Ukraini kriz pryzmu yevrointehratsiinykh benchmarkiv ta standartiv International IDEA [Delegated Legislation in Ukraine Through the Prism of European Integration Benchmarks and International IDEA Standards]. Prykarpatskyi iurydychnyi visnyk – Subcarpathian Law Bulletin. Issue 1 (66). P. 29–34. DOI https://doi.org/10.32782/pyuv.v1.2026.6

5. Konstytutsiia Ukrainy [Constitution of Ukraine]: Law of Ukraine of June 28, 1996 No. 254k/96-VR (1996). Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of the Verkhovna Rada of Ukraine. No. 30. Art. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

6. Kostiuk Yu. V., Skladannyi P. M., Hulak H. M., Bebeshko B. T., Khorolska K. V., Rzaieva S. L. (2025). Systemy zakhystu informatsii [Information Security Systems]: textbook. Kyiv: Kyivskyi stolichnyi universytet imeni Borysa Hrinchenka – Borys Grinchenko Kyiv Metropolitan University. 887 p. URL: https://elibrary.kubg.edu.ua/id/eprint/51359/1/Kostiuk_Y_Skladannyi_P_Hulak_H_Bebeshko_B_Khorolska_K_Rzaieva_S_SZI_2025_FITM.pdf.

7. Lysak S.-Iu. Yu. (2026). Antykoruptsiina polityka suchasnoi derzhavy: yevropeiski oriientyry ta napriamky rozvytku [Anti-Corruption Policy of the Modern State: European Orientations and Development Directions]. Prykarpatskyi iurydychnyi visnyk – Subcarpathian Law Bulletin. Issue 1 (66). P. 35–38. DOI https://doi.org/10.32782/pyuv.v1.2026.7

8. Mykhailyk A. S. (2021). Suchasnyi stan ta problemy zakhystu personalnykh danykh pratsivnykiv v Ukraini v umovakh tsyfrovoi transformatsii [Current State and Problems of Protection of Employees' Personal Data in Ukraine in the Conditions of Digital Transformation]. Sotsialne pravo – Social Law. No. 4. P. 200–207. URL: https://ir.library.knu.ua/handle/15071834/24866

9. Osyka Yu. V. (2023). Pravove rehuliuvannia vykorystannia personalnykh danykh [Legal Regulation of the Use of Personal Data]. Irpinskyi iurydychnyi chasopys – Irpin Law Journal. Issue 3 (12). P. 343–351. DOI 10.33244/2617-4154.3(12).2023.343-351

10. Rizenko, O. V. (2024). European legal standards for personal data protection. Analytical and Comparative Jurisprudence, (6), 643–648. DOI https://doi.org/10.24144/2788-6018.2024.06.105

11. Prystai R. A. (2024). Natsionalni orhany zakhystu danykh v Yevropeiskomu Soiuzi: rol i praktyka v sferi zakhystu personalnykh danykh v sotsialnykh merezhakh [National Data Protection Authorities in the European Union: Role and Practice in the Field of Personal Data Protection in Social Networks]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Scientific Bulletin of Uzhhorod National University. Series: Law. Issue 82 (2). P. 245–252. DOI https://doi.org/10.24144/2307-3322.2024.82.2.39

12. Pro zakhyst personalnykh danykh [On Personal Data Protection]: Law of Ukraine of June 01, 2010 No. 2297-VI (2010). Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of the Verkhovna Rada of Ukraine. No. 34. Art. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

13. Rizak M. V. (2018). Administratyvno-pravove zabezpechennia vidnosyn obihu ta obrobky personalnykh danykh v Ukraini [Administrative and Legal Support of Relations Governing the Circulation and Processing of Personal Data in Ukraine]: Extended abstract of Doctor of Sciences dissertation (12.00.07). Kharkiv: Kharkivskyi natsionalnyi universytet vnutrishnikh sprav – Kharkiv National University of Internal Affairs. 39 p. URL: https://dspace.univd.edu.ua/items/b86b4c7d-d0b7-460f-9c06-fd5095416024.

14. Roik M. (2023). Vidpovidnist zakonodavstva Ukrainy okremym polozhenniam pravovoho rehuliuvannia sfery vidkrytykh danykh u Yevropeiskomu Soiuzi [Compliance of Ukrainian Legislation with Certain Provisions of Legal Regulation of Open Data in the European Union]: Analytical Report. Ed. O. Zaiarnyi. Kyiv: Ministerstvo tsyfrovoi transformatsii Ukrainy – Ministry of Digital Transformation of Ukraine. 31 p. URL: https://eef.org.ua/wp-content/uploads/2023/07/Vidpovidnist-zakonodavstva-Ukrayiny-okremym-polozhennyam-pravovogo-regulyuvannya-sfery-vidkrytyh-danyh-u-YEvropejskomu-Soyuzi.pdf.

15. APD/GBA. (2020). Beslissing ten gronde / Décision quant au fond n° 25/2020 du 14 mai 2020. Autorité de protection des données. URL: https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/Beslissing_GK_25-2020_EN.pdf

16. Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 1 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist. URL: https://www.gesetze-im-internet.de/bdsg_2018/

17. CNIL. (2025). Publicités insérées entre les courriels et cookies : la CNIL sanctionne GOOGLE d'une amende de 325 millions d'euros. Paris: Commission Nationale de l'Informatique et des Libertés, September 03, 2025. URL: https://www.cnil.fr/fr/thematique/cnil/sanctions.

18. European Data Protection Board. (2023). Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 2.1. Brussels: EDPB.

19. General Data Protection Regulation (GDPR). (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union. L 119. P. 1–88. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504.

20. GDPR Enforcement Tracker. (2023). Report. CMS Law. Fine ID: ET-2212 (TikTok Technology Limited). URL: https://www.enforcementtracker.com/

21. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

22. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dz.U. 2018 poz. 1000. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000

23. Korchynskyi D., Kobrin A., Nekrutenko V. (2020). Ukrainian GDPR: The reality and future of privacy legislation in Ukraine. IAPP, September 28, 2020. URL: https://iapp.org/news/a/ukrainian-gdpr-the-reality-and-future-of-privacy-legislation-in-ukraine.

24. Stratonov V. M., Savielieva I. V. (2020). Okremi aspekty vykorystannia biometrychnykh personalnykh danykh u profilaktytsi pravoporushen [Certain Aspects of the Use of Biometric Personal Data in Crime Prevention]. Iurydychnyi biuleten – Legal Bulletin. Issue 16. P. 265–271. DOI https://doi.org/10.32850/LB2414-4207.2020.16.35

25. Stratonov V., Konovalova V., Savelieva I. (2021). Biometric personal data and their use in the investigation of criminal offences. Journal of the National Academy of Legal Sciences of Ukraine. Vol. 28, No. 4. DOI https://doi.org/10.24144/2307-3322.2024.82.2.39

Дата першого надходження статті до видання: 04.09.2026
Дата прийняття статті до друку після рецензування: 01.10.2026
Дата публікації (оприлюднення) статті: 09.11.2026