

УДК 342

DOI <https://doi.org/10.24144/2307-3322.2025.90.3.30>

ЗАХИСТ ІНФОРМАЦІЙНИХ ПРАВ ОСОБИ В УМОВАХ ЦИФРОВІЗАЦІЇ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: ТЕОРЕТИКО-ПРАВОВИЙ АСПЕКТ

Калюжний Д.,
*здобувач вищої освіти третього (наукового) рівня
Національного аерокосмічного університету
«Харківський авіаційний інститут»
ORCID: 0009-0006-1709-8405/print
e-mail: dmitriykoluznyj555@gmail.com*

Калюжний Д. Захист інформаційних прав особи в умовах цифровізації правоохоронної діяльності: теоретико-правовий аспект.

Стаття присвячена комплексному дослідженню правових аспектів захисту інформаційних прав особи в умовах цифровізації правоохоронної діяльності. Акцентовано, що активне впровадження інформаційно-комунікаційних технологій у роботу органів правопорядку значно підвищує ефективність виконання завдань з підтримання правопорядку та безпеки, однак водночас формує нові виклики для реалізації конституційного права на приватність та належного захисту персональних даних. Проаналізовано положення Конституції України, Закону України «Про захист персональних даних», а також міжнародно-правові акти – Конвенцію Ради Європи 108+ та Загальний регламент ЄС про захист даних (GDPR), що визначають стандарти та гарантії у сфері обробки конфіденційної інформації. Окремо розглянуто колізії та прогалини чинного законодавства, серед яких – відсутність чітко врегульованих процедур доступу до персональних даних, недостатня незалежність механізмів контролю за їх обробкою та низький рівень цифрової компетентності окремих категорій працівників правоохоронних органів.

У роботі приділено увагу проблемі забезпечення балансу між потребами національної безпеки та дотриманням прав і свобод людини. Детально розкрито застосування принципів законності, пропорційності та прозорості при зборі, зберіганні, передачі й використанні персональних даних у правоохоронній сфері.

На основі проведеного аналізу сформульовано пропозиції щодо вдосконалення правового регулювання, зокрема: запровадження детальніших процедур доступу до даних, використання сучасних технологій криптографічного захисту, посилення інституційного та громадського контролю, а також систематичного підвищення кваліфікації правоохоронців у сфері цифрової безпеки.

Отримані результати можуть бути використані для подальших наукових досліджень, розробки проектів нормативно-правових актів та вдосконалення практичної діяльності органів правопорядку з урахуванням вимог захисту прав людини у цифровому середовищі.

Ключові слова: правоохоронна діяльність, інформаційно-комунікаційні технології, інформаційні права, інформаційна безпека, інформаційні права, захист персональних даних, правоохоронні органи, правове регулювання.

Kaliuzhnyi D. Protection of individual information rights in the context of digitalisation of law enforcement: theoretical and legal aspects.

The article is devoted to a comprehensive study of the legal aspects of protecting individuals' information rights in the context of the digitalization of law enforcement activities. It emphasizes that the active implementation of information and communication technologies in the work of law enforcement agencies significantly increases the effectiveness of maintaining public order and security; however, it simultaneously creates new challenges for the realization of the constitutional right to privacy and the proper protection of personal data. The analysis covers the provisions of the Constitution of Ukraine, the Law of Ukraine "On Personal Data Protection," as well as international legal instruments – the Council

of Europe Convention 108+ and the EU General Data Protection Regulation (GDPR), which set out standards and guarantees in the field of confidential information processing. Particular attention is given to conflicts and gaps in the current legislation, including the absence of clearly regulated procedures for access to personal data, insufficient independence of mechanisms controlling data processing, and the low level of digital competence among certain categories of law enforcement personnel.

The study also addresses the issue of balancing national security needs with respect for human rights and freedoms. It elaborates on the application of the principles of legality, proportionality, and transparency in the collection, storage, transfer, and use of personal data in the law enforcement sector.

Based on the analysis, the article formulates proposals for improving legal regulation, including: introducing more detailed procedures for data access, applying modern cryptographic protection technologies, strengthening institutional and public oversight, and systematically enhancing the digital security competencies of law enforcement officers.

The findings may be used for further academic research, the development of draft legislative acts, and the improvement of law enforcement practices in compliance with human rights protection requirements in the digital environment.

Key words: law enforcement, information and communication technologies, information rights, information security, information rights, personal data protection, law enforcement agencies, legal regulation.

Постановка проблеми. В сучасних умовах цифрової трансформації державного управління та правоохоронної системи проблема захисту інформаційних прав особи набуває особливої актуальності. Правоохоронні органи дедалі активніше використовують інформаційно-комунікаційні технології (ІКТ) для реалізації своїх функцій: збору доказів, здійснення моніторингу, аналізу поведінкових даних, контролю за переміщенням осіб тощо. Ці процеси безпосередньо пов'язані з обробкою великого масиву персональних даних громадян, що створює ризики порушення їхніх основоположних прав і свобод, зокрема – права на приватність, захист персональної інформації та свободу вираження поглядів.

Недостатня прозорість цифрових механізмів, відсутність належного контролю за їх використанням, а також фрагментарне правове регулювання вказують на потребу доктринального осмислення меж допустимого втручання держави в інформаційний простір особи. У цьому контексті важливо визначити теоретико-правову природу інформаційних прав, засади їх реалізації та захисту у взаємодії з правоохоронною системою, яка в умовах цифровізації отримує значний обсяг владних повноважень щодо доступу до приватної інформації.

Правоохоронна діяльність за своєю суттю передбачає втручання в особисте життя людини, однак таке втручання має здійснюватися з дотриманням чітко встановлених меж. Порушення інформаційних прав – особливо у контексті збору, обробки та зберігання персональних даних – створює ризики надмірного державного контролю, порушення права на приватність, обмеження свободи вираження поглядів і пересування.

Сучасне українське законодавство лише частково враховує особливості цифрового виміру правоохоронної діяльності. Нерідко норми носять декларативний характер, не мають належного механізму реалізації та залишають простір для зловживань. У зв'язку з цим виникає потреба у комплексному науковому аналізі правового забезпечення інформаційних прав громадян у діяльності правоохоронних органів, з урахуванням стрімкого розвитку ІКТ, широкого використання їх у правоохоронній діяльності та міжнародних стандартів захисту персональних даних.

Стан опрацювання. Проблематика інформаційних прав у загальному вигляді розглядається у працях українських і зарубіжних науковців, зокрема з позицій права на інформацію, права на захист персональних даних, інформаційної безпеки, цифрової етики тощо. Серед вітчизняних дослідників варто виокремити праці: В. Цимбалюка та В. Шемчук – щодо конституційно-правових гарантій інформаційної безпеки особи; С. Гуцу та П. Дуравкін – у сфері цифрових прав людини в умовах трансформації інформаційного суспільства; Т. Попович, Я. Худолей, Н. Загребельна – щодо проблем правового регулювання захисту персональних даних; Ю. Тимошенко та В. Василенко про юридичні аспекти використання ІКТ у правоохоронній діяльності.

На міжнародному рівні особливого значення набули дослідження, присвячені реалізації стандартів GDPR [8], Конвенції 108+ [5], а також практиці Європейського суду з прав людини щодо права на приватне життя (зокрема рішення у справах *Zakharov v. Russia*, *S. and Marper v. UK*, *Big Brother Watch v. UK*) [11-14].

Водночас, у вітчизняному науковому просторі ще недостатньо розробленою залишається системна оцінка:

- співвідношення потреби у безпеці та захисту персональних даних у правоохоронній сфері;
- меж допустимого втручання держави в інформаційні права громадян;
- процесуальні норми законного використання технологій при роботі з інформацією і даними;
- процедурних гарантій при роботі з персональними даними.

Це й обумовлює актуальність запропонованого дослідження.

Метою дослідження є формулювання теоретико-правових основ захисту інформаційних прав особи в умовах цифровізації правоохоронної діяльності, виявлення правових ризиків, аналіз механізмів гарантування інформаційної безпеки громадян, а також розробка пропозицій щодо вдосконалення законодавства у цій сфері.

Виклад основного матеріалу. У контексті цифровізації суспільства, питання забезпечення інформаційних прав громадян набуває особливої актуальності. Інформаційні права є складовою частиною фундаментальних прав і свобод людини, гарантованих як національним, так і міжнародним правом, і набувають нових змістовних аспектів у зв'язку з розвитком інформаційно-комунікаційних технологій (ІКТ) та використанням їх у правоохоронній діяльності.

Поняття «інформаційні права» охоплює низку юридичних гарантій, що забезпечують особі право вільно отримувати, зберігати, поширювати та захищати інформацію. В українському законодавстві ключові положення щодо інформаційних прав закріплено у Конституції України (ст. 32, 34), Законі України «Про інформацію» [3], Законі України «Про захист персональних даних» [2] та інших нормативно-правових актах. Так, відповідно до статті 32 Конституції України, не допускається втручання в особисте і сімейне життя особи, крім випадків, передбачених законом [7]. Також гарантується судовий захист права кожного на невтручання в його особисте життя, таємницю кореспонденції, телефонних розмов, телеграфної та іншої кореспонденції. У сфері кримінального провадження особливе значення має Кримінальний процесуальний кодекс України, який регулює доступ до інформації в рамках слідчих дій.

Правове регулювання у сфері персональних даних в Україні базується на Законі України «Про захист персональних даних» [2], який встановлює принципи обробки, права суб'єкта даних та обов'язки володільців і розпорядників. Разом із тим, специфіка правоохоронної діяльності потребує окремого підходу до врегулювання повноважень правоохоронців в сфері захисту інформаційних прав і свобод людини.

На міжнародному рівні, ключове значення має стаття 8 Конвенції про захист прав людини і основоположних свобод [4], яка встановлює право кожного на повагу до приватного життя, житла, кореспонденції, за винятком обмежень, передбачених законом і необхідних у демократичному суспільстві.

Особливої уваги заслуговує Конвенція Ради Європи № 108+ про захист осіб у зв'язку з автоматизованою обробкою персональних даних [5] та Загальний регламент про захист даних (GDPR) [8], що діє в Європейському Союзі. Ці документи формують стандарти захисту персональних даних, обов'язкові не лише для суб'єктів приватного сектору, але й для правоохоронних органів, які здійснюють обробку персональних даних у рамках кримінального провадження, профілактики правопорушень або забезпечення національної безпеки. Незважаючи на прийняті нормативні акти, проблема захисту інформаційних прав залишається актуальною на фоні постійного і динамічного розвитку технологій і використання їх в діяльності правоохоронних органів.

Розуміння сутності інформаційних прав дозволяє більш чітко окреслити межі допустимого втручання держави у приватне життя особи у цифровому середовищі, а також визначити правові засоби захисту від зловживань з боку правоохоронців.

Інформаційні права є складовою частиною основоположних прав і свобод людини, що передбачають можливість особи вільно шукати, отримувати, використовувати та поширювати інформацію, а також захищати свою інформаційну автономію. До таких прав належить право на приватність, захист персональних даних, право на інформування, доступ до публічної інформації тощо. [10] Зазначені права тісно взаємопов'язані: реалізація права на доступ до інформації не повинна порушувати право на приватність; у свою чергу, обмеження права на приватність можливе лише за умов законного, необхідного і пропорційного втручання, зокрема – у сфері правоохоронної діяльності.

Інформаційні права мають універсальний характер і підлягають захисту в будь-якому контексті, включаючи взаємодію громадян із правоохоронними органами.

Інформаційні права є інтегрованою частиною системи прав людини, забезпечення яких є обов'язком демократичної держави. Їх порушення в умовах цифрової взаємодії часто має системний характер і тягне за собою широкі наслідки – як для окремої особи, так і для суспільства в цілому. У цьому сенсі особливе значення має правове регулювання діяльності органів публічної влади, зокрема правоохоронних структур, з урахуванням стандартів прав людини.

Правоохоронні органи дедалі активніше впроваджують інформаційно-комунікаційні технології у свою діяльність. Це включає використання електронних баз даних, систем відеоспостереження, розпізнавання облич, геолокаційного моніторингу, електронного документообігу та навіть штучного інтелекту для аналізу поведінкових моделей. З одного боку, цифрові інструменти забезпечують оперативність розслідувань, аналітичність та інтегрованість правоохоронної діяльності, дозволяють ефективніше здійснювати превентивні заходи, розкривати злочини, оптимізувати обмін інформацією між відомствами. З іншого – вони створюють умови для масового збору інформації про осіб без їх згоди, що загрожує приватності.

Особливе занепокоєння у правозахисників викликають:

- автоматизовані системи обліку громадян;
- взаємодія з телекомунікаційними операторами щодо отримання даних про дзвінки, повідомлення, геолокацію;
- розширення функціоналу систем відеоспостереження з функцією розпізнавання осіб.

Відсутність чітких стандартів та прозорих процедур у роботі з цифровими даними призводить до ризиків порушення прав громадян. [9] Національне законодавство не повністю враховує сучасні виклики, пов'язані з автоматизованою обробкою інформації в правоохоронній сфері. Бракує чітких процедур доступу, обмеження, моніторингу та відповідальності за зловживання.

Одним з головних викликів цифровізації є збереження балансу між потребою держави в ефективному реагуванні на загрози безпеці та забезпеченням гарантій непорушності особистого простору громадян. Надмірне посилення контролю – наприклад, шляхом масового відеоспостереження, розпізнавання облич, біометричної ідентифікації – може спричинити перетворення правоохоронної системи з інструменту безпеки на механізм масового нагляду. Концепція правомірного втручання передбачає, що обмеження прав можливі лише: на підставі закону; з легітимною метою (захист безпеки, правопорядку) та за умови необхідності та пропорційності втручання.

У демократичному суспільстві питання «безпека чи свобода» не має однозначної відповіді. Законодавець повинен забезпечити:

- чітке регулювання повноважень правоохоронних органів у сфері збору та обробки даних;
- впровадження незалежного нагляду за їхньою діяльністю (наприклад, через інститути омбудсмена або парламентський контроль);
- ефективні засоби юридичного захисту особи у випадках порушення її інформаційних прав;
- відповідальність посадових осіб за зловживання цифровими інструментами у правоохоронній сфері.

Таким чином, на теоретико-правовому рівні захист інформаційних прав особи у правоохоронній діяльності має базуватися на зваженому співвідношенні інтересів особи та інтересів держави, із пріоритетом людської гідності та прав людини як вищих соціальних цінностей. Повноваження правоохоронних органів у сфері персональних даних мають бути чітко визначені законом. Доступ до даних повинен ґрунтуватися на судовому дозволі, містити обґрунтування мети і бути пропорційним.

Прецеденти Європейського суду (наприклад, «S. and Marper v. the UK», «Roman Zakharov v. Russia») демонструють жорсткі вимоги до законності збору інформації. Згідно з усталеною практикою Європейського суду з прав людини, втручання органів державної влади у приватне життя допускається лише за наявності законної мети, правового підґрунтя та необхідності у демократичному суспільстві. Це означає, що будь-яке обмеження інформаційних прав має бути пропорційним та обґрунтованим.

Правоохоронні органи зобов'язані діяти у межах повноважень, передбачених законом, не виходити за рамки визначених процедур та уникати надмірного збору, зберігання чи поширення персональної інформації без належного обґрунтування.

Крім цього, слушною є пропозиція запровадження прозорих процедур контролю та аудиту доступу до персональних даних. [6] Повинні бути розроблені механізми фіксації запитів правоохоронних органів до інформаційних систем, автоматизовані журнали аудиту, обов'язкова звітність, участь органів незалежного нагляду. Необхідно встановити процедури обліку доступів до даних, створити інструменти аудиту цифрових дій правоохоронців, а також забезпечити зовнішній контроль (наприклад, незалежними комісіями чи омбудсменом).

Важливим елементом в питанні додержання інформаційних свобод громадян є належна підготовка кадрів та розвиток цифрової і правової культури правоохоронців. Захист прав особи має бути вплетений у професійні стандарти роботи правоохоронців. Це потребує системної підготовки, перепідготовки кадрів, включення інформаційної етики в навчальні програми та службові інструкції.

Висновки. В умовах цифровізації правоохоронної діяльності існує об'єктивна потреба у переосмисленні підходів до забезпечення інформаційних прав особи. У сучасних умовах цифровізації інформаційні права громадян є одним із найбільш уразливих елементів правового статусу особи. Правоохоронні органи, виконуючи завдання із забезпечення публічного порядку та безпеки, зобов'язані діяти у правовому полі, дотримуючись принципів законності, пропорційності та мінімального втручання. Ефективний правовий захист передбачає як оновлення нормативної бази, так і зміну управлінських, організаційних і освітніх практик. Удосконалення національного законодавства відповідно до норм GDPR та Конвенції 108+ дозволить забезпечити системність та юридичну визначеність у сфері обробки даних. Актуальною є ідея розробки окремого нормативного акту щодо цифрових прав у кримінальному провадженні, який би встановлював спеціальні гарантії захисту особи. Правоохоронці мають отримувати фахову підготовку з цифрової етики, кібербезпеки та прав людини в ІКТ-контексті.

Подальші наукові дослідження мають бути спрямовані на побудову моделі збалансованої взаємодії між технологіями безпеки та правами людини. Це стане запорукою довіри суспільства до правоохоронної системи та реальним інструментом зміцнення правової держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Закон України «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>.
2. Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
3. Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
4. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 року. URL: <https://www.echr.coe.int>.
5. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+) від 18 травня 2018 року. URL: <https://rm.coe.int/16808ade9d>.
6. Кондратенко В.М., Сокурено О.А. Адміністративно-правові засади забезпечення інформаційної безпеки та доступу до публічної інформації в діяльності правоохоронних органів сектору національної безпеки. *Науковий вісник Ужгородського Національного університету*, 2025. Серія ПРАВО. Випуск 89: частина 2. С. 452–457. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/07/71.pdf>.
7. Конституція України від 28 червня 1996 року № 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>.
8. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради (Загальний регламент про захист даних – GDPR) від 27 квітня 2016 року. URL: <https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=celex:32016R0679>.
9. Спіцина Г.О., Гуцу С.Ф. Легалізація поняття інформаційної безпеки особистості в українському законодавстві. Пропілеї права та безпеки : наук. журнал / Ред. кол. Н.Є. Філіпенко, І.Р. Шинкаренко, С.Ю. Лукашевич, та ін. Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», 2023. №. 2-3. С. 37–41.

10. Спіцина Г.О., Гуцу С.Ф. Щодо питання правового захисту персональних даних працівників. *Науковий вісник Ужгородського національного університету*. Серія ПРАВО. 2023. Випуск 76. Ч.1. С. 255–260.
11. Case of Big Brother Watch and Others v. the United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15), Judgment of 25 May 2021. European Court of Human Rights. URL: [https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-210077%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-210077%22]).
12. Case of Roman Zakharov v. Russia (Application no. 47143/06), Judgment of 4 December 2015. European Court of Human Rights. URL: [https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-159324%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-159324%22]).
13. Case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04), Judgment of 4 December 2008. European Court of Human Rights. [https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-90051%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-90051%22]).
14. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Council of Europe, 28 January 1981. URL: <https://www.coe.int/en/web/data-protection/convention108>.