МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

СОЦІАЛЬНО-ПОЛІТИЧНА ТА ПРАВОВА СИСТЕМА УКРАЇНИ В ЦИФРОВУ ЕПОХУ: СУЧАСНІ ВИКЛИКИ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 22 квітня 2026 року

Том 2

Одеса
2026

УДК 34:004:316.4(477)
С 70

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 23.04.2026 р.)

За загальною редакцією академіка ***С. В. Ківалова***

С70 **Соціально-політична та правова система України в цифрову епоху**: сучасні виклики : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 22 квітня 2026 р.) / заг. ред. С. Ківалова ; НУ «Одес. юрид. академія». – Одеса : Фенікс, 2026. – Т. 2. – 684 с.

ISBN 978-617-8763-16-9

Матеріали конференції узагальнюють результати наукових досліджень і практичних напрацювань учених, фахівців та представників професійних спільнот, виконаних в умовах воєнного часу та глибоких суспільних трансформацій.

У збірнику представлено широкий спектр наукових розвідок і практико-орієнтованих досліджень, що охоплюють актуальні проблеми публічного та приватного права, функціонування держави, судової та правоохоронної системи, а також трансформації суспільних процесів у цифрову епоху. Значну увагу приділено питанням адміністративного, фінансового, конституційного, міжнародного, морського та митного права, а також сучасним викликам у сфері кримінального права, кримінального процесу, криміналістики та оперативно-розшукової діяльності.

Окремі наукові секції присвячені проблемам удосконалення судоустрою, діяльності прокуратури, адвокатури та інших правоохоронних органів, розвитку трудового права і права соціального забезпечення, а також реформуванню цивільного, господарського, земельного, екологічного та енергетичного права. Збірник відображає також міждисциплінарний характер сучасних досліджень, охоплюючи питання філософії права, світових соціально-політичних процесів, соціології та психології, економіки та підприємництва в умовах війни і повоєнного відновлення. Важливе місце посідають дослідження у сфері інформаційних технологій, кібербезпеки, штучного інтелекту та математичного моделювання як ключових чинників забезпечення національної безпеки.

Крім того, у збірнику висвітлено проблематику педагогіки, лінгвістики права, перекладознавства, журналістики, фізичної та військової підготовки здобувачів вищої освіти.

Збірник розрахований на науковців, викладачів, здобувачів вищої освіти та практиків у галузях права, економіки, соціології, психології, політології, інформаційних технологій і суміжних дисциплін.

УДК 34:004:316.4(477)

Відповідальний за випуск професор ***М. Р. Аракелян***

Матеріали видано в авторській редакції.

ISBN 978-617-8763-16-9

Задерейко Олександр Владиславович
Національний університет «Одеська юридична академія»,
доцент кафедри штучного інтелекту та математичного моделювання,
кандидат технічних наук, доцент
Єленич Світлана Іграфівна
Національний університет «Одеська юридична академія»,
головний бібліограф наукової бібліотеки

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ СУБ'ЄКТІВ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА

В законодавстві України та країн Європейського Союзу використовується типове формулювання поняття «персональні дані». Це «дані або інформація про особу, яку можна ідентифікувати». Іноді використовується формулювання з невеликими змінами, що «персональні дані це дані, які дозволяють прямо чи опосередковано ідентифікувати особу» [1; 2]. Незважаючи на схожість формулювань, закони по-різному трактують те, що дійсно підпадає під їх захист. У деяких країнах прямо перераховують категорії персональних даних, які підпадають під їх захист. Це означає, що навіть там, де офіційні формулювання, на думку законодавців, чітко визначені, розвиток інформаційних технологій може, за фактом, «доповнювати» їх перелік. «Гнучкі» формулювання, в свою чергу, дозволяють адаптуватися до майбутніх змін, але при цьому створюють невизначеність. Дані, які не входять до складу персональних даних, вважаються «не персональними даними». Такий статус позбавляє їх якщо не повністю, то здебільшого захисту з боку закону. Така концепція стала застосовуватись до «знеособлених» даних, з яких навмисно була видалена ідентифікуюча особу інформація.

Перелік персональних даних в національному законодавстві країн може бути різний. В Україні перелік конфіденційної інформації охоплює дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адресу, дату і місце народження [3].

Увага дослідників зосереджена на класифікації персональних даних / конфіденційної інформації у поєднанні із збереженням права людини на приватність та гарантуванням високого рівня захищеності від кібератак. У публікації [4] конфіденційна інформація, що потребує захисту, була впорядкована за такими критеріями: 1) за правом власності: а) державна; б) приватна; 2) за правом доступу: а) під час виконання посадовими особами службових повноважень; б) власника та осіб, яким надано це право; 3) за галуззю застосування: а) комерційна; б) банківська; в) податкова; г) адвокатська; д) судова тощо.

Інший підхід класифікації персональних даних пропонується у дослідженні [5]. Автори розподіляють персональні дані в залежності від: – сфери використання (персональні дані працівників та публічних осіб, а також ті персональні дані, що використовуються у цифровому середовищі тощо); – можливості поширення (відкриті та конфіденційні персональні дані); – відношення до приватно-

сті особи (звичайні та чутливі персональні дані); – підстав та мети їх обробки; – рівня захищеності персональних даних в залежності від правового режиму, що вводиться в Україні.

Для системи безпеки [6] важливим є розподіл інформації за рівнем критичності наслідків, спричинених втратою стратегічних та секретних даних (1 рівень), конфіденційних даних (2 рівень), внутрішніх даних (3 рівень), публічних даних (4 рівень). Наприклад, викрадення критичної інформації другого рівня, до яких автори публікації відносять персональні дані, комерційну таємницю, інформацію про клієнтів та партнерів призведуть до значних фінансових втрат, репутаційних збитків, судових позовів та штрафів.

Аналіз актуальних досліджень демонструє наскільки різними можуть бути підходи до систематизації персональних даних, розмежування яких здійснюється за ознаками та властивостями, цільовим призначенням оброблення даних та наслідками для інформаційного суверенітету держави від їх втрати.

Цифрові відносини між державою та громадянами базуються на системі електронної ідентифікації фізичних осіб [7]. Процес ідентифікації реалізується шляхом обробки унікальних атрибутів суб'єкта, до яких належать біометричні шаблони, автентифікаційні пари (логін/пароль), електронні ідентифікаційні документи та засоби кваліфікованого електронного підпису. Зазначені дані виступають базисом для формування цифрового профілю – структурованого набору атрибутів, що забезпечує авторизований доступ до електронних сервісів, платформ електронної комерції та соціальних мереж.

У межах взаємодії в цифровому середовищі верифікація трактується як процедура встановлення коректності зв'язку між цифровим профілем та його носієм – фізичною особою. Ідентифікація особи ґрунтується на застосуванні трьох категорій даних:

- персональних даних, які розмежовуються на конфіденційну та публічну інформацію;
- технічних даних, що фіксуються в процесі взаємодії суб'єкта з інформаційно-комунікаційними системами (метадані, ідентифікатори, параметри сеансів тощо);
- криптографічних ідентифікаторів, що забезпечують цілісність та невід'ємність автентифікаційних транзакцій.

Ідентифікація користувача у цифровому середовищі формується як сукупність стійких ідентифікаторів, які дозволяють однозначно розрізняти суб'єктів шляхом створення багатошарової моделі з використанням явних ідентифікаторів кожного комунікаційного пристрою. До них відносяться:

- логін/username;
- адреса електронної пошти;
- номер телефону;
- обліковий запис у сервісі (наприклад, Google Account, Apple ID);
- візуальні образи в акаунтах (зображення, аватар);

- біометрія (відбиток пальця, Face ID);
- IP-адреса;
- MAC-адреса модуля мережевої комунікації;
- device ID (Android ID, IDFA та інші);
- cookies та session ID;
- user-agent (браузер, операційна система, версія);
- відвідані мережеві адреси (URL вебсторінки, доменні імена).

У межах взаємодії суб'єкта з інформаційно-комунікаційними системами технічні вище зазначені дані комунікаційного пристрою, набувають статусу об'єктів підвищеного захисту. Це зумовлено тим, що зазначені атрибути у своїй сукупності уможливлюють встановлення кореляції між діяльністю користувача у цифровому середовищі та його фізичною ідентичністю. Відтак всі перелічені ідентифікатори слід розглядати як складові персональних даних у структурі цифрового профілю особи.

Окрім безпосередньої ідентифікації, такі дані здатні опосередковано персоналізувати особу – через їх поєднання з іншими відомостями, що формують унікальний цифровий профіль її комунікаційного пристрою. Саме ця властивість зумовлює актуальність проблематики захисту персональних даних у контексті запобігання їх несанкціонованому доступу, модифікації, втраті, вилученню чи знищенню. Чинником вразливості персональних даних виступає будь-який окремий їх фрагмент, будучи співставленним із додатковими даними, може призвести до втрати приватності особи. У цьому сенсі навіть гіпотетична можливість непрямої ідентифікації є достатньою підставою для застосування до таких даних режиму захисту.

У процесі комунікації особи з цифровим середовищем відбувається акумуляція значних масивів даних, що фіксують її взаємодію з різноманітними онлайн-сервісами. Характерною особливістю сучасного стану відносин у цифровому просторі є фактична відсутність у користувачів ефективних важелів заборони на збір їх персональних даних. Згодом бази даних, що містять цифрові профілі комунікаційних пристроїв осіб, можуть бути надані третім сторонам для спільного використання, що призводить до ідентифікації їхніх користувачів.

Створення цифрових профілів користувачів комунікаційних пристроїв є набагато ефективнішим, ніж стеження за ними іншими доступними способами. Фактично такий «профіль» не можна видалити – можна лише ввести в оману системи аналізу (надати йому інший ідентифікатор).

Унікальні цифрові профілі пристроїв комунікації можуть бути використані для:

- збору даних про відвідування певних інтернет-ресурсів та дій користувача на них;
- налаштування персоналізованої реклами що базується на прихованих інтересах користувача;
- стеження за користувачами в інших цілях.

Небезпека полягає в систематичному зростанні обсягу електронної персоналізованої інформації про особу. Її поглиблений аналіз дозволяє викривати приховані патерни поведінки, будувати прогнози, а при системній роботі – цілеспрямовано корегувати поведінкові тренди для всі користувачів цифрового середовища. Зазначені ризики формують запит на надійний захист суб'єктів цифрового простору від будь-якого використання їх даних.

Список використаних джерел:

1. Про захист персональних даних : закон України від 01 черв. 2010 р. № 2297-VI. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17# Text
2. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 р. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text, https://gdpr-text.com/.
3. Про інформацію : закон України від 02 жовт. 1992 р. № 2657-XII. *Офіційний сайт Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
4. Ярмакі Х. П., Музика С. С. Класифікація конфіденційної інформації. *Південноукраїнський правничий часопис*. 2021. № 1. С. 94-98. DOI: https://doi.org/10.32850/sulj.2021.1.16
5. Пальчик М. Л., Шкрібляк К. П., Березделцький Ю. М. Актуальні проблеми захисту персональних даних як напряму забезпечення національної безпеки України в умовах війни. *Аналітично-порівняльне правознавство*. 2025. Вип. 6, ч. 2. С. 425-434. DOI: https://doi.org/10.24144/2788-6018.2025.06.2.69
6. Івкова В. С., Опірський І. Р. Дослідження існуючих засобів та підходів до проведення OSINT в контексті інформаційної безпеки особи та держави. *Комп'ютерні системи та мережі*. 2025. Вип. 7. № 1. С. 143-159. DOI: https://doi.org/10.23939/csn2025.01.131
7. Задерейко О. В., Трофименко О. Г., Єленич С. І., Логінова Н. І., Гура В. І. Системний аналіз захищеності державних електронних реєстрів та баз персональних даних. *Кібербезпека: освіта, наука, техніка*. 2025. № 4(28). С. 57-70. DOI: https://doi.org/10.28925/2663-4023.2025.28.735

Ключові слова: комунікаційні пристрої, цифровий профіль, персональні дані, ідентифікація у цифровому середовищі, ідентифікатори комунікаційного пристрою.

Key words: communication devices, digital profile, personal data, digital identification, communication device identifiers.

Наукове видання

СОЦІАЛЬНО-ПОЛІТИЧНА ТА ПРАВОВА СИСТЕМА УКРАЇНИ В ЦИФРОВУ ЕПОХУ: СУЧАСНІ ВИКЛИКИ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 22 квітня 2026 року

Том 2

За загальною редакцією ***С. В. Ківалова***

Відповідальний за випуск ***М. Р. Аракелян***

Підписано до друку 05.05.2026.
Формат 60х84/16. Ум-друк. арк. 39,76.
Наклад 100 прим. Зам. № 2605-02.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net