

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Кафедра цивільного права

ІТ-ПРАВО ТА КІБЕРБЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ

**МАТЕРІАЛИ
Всеукраїнського круглого столу**

Одеса,
12 квітня 2025 року

Одеса
Фенікс
2025

УДК 342.95 : 343.32 (477): 351.863
I-52

За загальною редакцією

доктора юридичних наук, професора **Є. Харитонова**,
кандидатки юридичних наук, доцентки **Ю. Кривенко**.

Упорядники-укладачі:

Кривенко Юлія – к.ю.н., доцентка кафедри цивільного права Національного університету «Одеська юридична академія», доцентка;

Лешкова Єлизавета – лаборантка кафедри цивільного права Національного університету «Одеська юридична академія».

ІТ-право та кібербезпека в умовах гібридної війни :
I-52 матеріали Всеукр. круглого столу (м. Одеса, 12 квіт. 2025 р.) / за заг. ред.: Є. О. Харитонова, Ю. Кривенко ; кафедра цив. права НУ «Одес. юрид. академія». – Одеса : Фенікс, 2025. – 138 с. – Режим доступу:

ISBN 978-617-8430-57-3

Збірник містить матеріали доповідей з теоретичних, історичних і методологічних проблем ІТ-права та кібербезпеки, які були оприлюднені на Всеукраїнському круглому столі «ІТ-право та кібербезпека в умовах гібридної війни» 12 квітня 2025 у Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення громадськості з дослідженнями науковців у сфері ІТ-права та кібербезпеки і може бути корисний як у навчальному процесі, так і в практичній діяльності.

УДК 342.95 : 343.32 (477): 351.863

*Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть
учасники конференції, їхні наукові керівники, рецензенти,
які рекомендували ці матеріали до друку.*

ISBN 978-617-8430-57-3

© Колектив авторів, 2025

© НУ «Одеська юридична академія»,
2025

Мурашева Катерина Василівна,
*студентка 2-го курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц., доц. кафедри цивільного права
Завальнюк С. В.*

ПЕРСОНАЛЬНІ ДАНІ ТА ЇХ ЗАХИСТ: ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ В УМОВАХ КІБЕРЗАГРОЗ

Розвиток інформаційних технологій в сучасному суспільстві приносить багато користі різним сферам життя, але і ускладнює життя новими викликами. Тема кіберзагроз, після кібератаки на державні реєстри України – хакерські атаки на сайти Національних інформаційних систем та Міністерства юстиції України, актуальна як ніколи. Актуальними є також проблеми правового регулювання персональних даних у цивільно-правовому вимірі в умовах кіберзагроз, а саме: збільшення масштабів кібератак – безперервне вдосконалення методів атак та недосконалість систем безпеки становлять загрозу конфіденційності персональних даних; труднощі з ідентифікацією відповідальності – складність визначення відповідального за витік чи неправомірне використання даних у випадку кібератак або неналежного захисту інформації; недостатня дієвість механізмів захисту прав суб'єктів персональних даних – ускладнена процедура подання скарг і притягнення до відповідальності порушників; юридична відповідальність за порушення – неефективність санкцій та відсутність дієвих механізмів притягнення до відповідальності за незаконну обробку персональних даних.

Визначення персональних даних згідно з національним та міжнародним законодавством можна трактувати так:

Персональні дані – це будь-яка інформація, що стосується ідентифікованої або такої, що може бути ідентифікована, фізичної особи (суб'єкта персональних даних). Вони можуть містити ім'я, дату народження, адресу, номер телефону, електронну пошту, ідентифікаційний код, біометричні та генетичні дані тощо. Відповідно до міжнародного законодавства, зокрема Загального регламенту про захист даних Європейського Союзу, персональні дані охоплю-

ють будь-яку інформацію, що прямо чи опосередковано стосується фізичної особи. Схоже визначення надає Конвенція № 108 Ради Європи [5]. В Україні регулювання у сфері захисту персональних даних відбувається згідно з Законом України «Про захист персональних даних». [2]Згідно з цим законом, персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Обов'язки що полягають на суб'єктів для обробки персональних даних (контролерів і процесорів) містять: обробку даних відповідно до принципів законності, прозорості та добросовісності; захист даних від несанкціонованого доступу, втрати чи пошкодження; виконання вимог законодавства щодо згоди на обробку даних; надання особам можливості реалізовувати свої права на захист даних [7].

Цивільно-правовий захист персональних даних є важливим елементом сучасного правового регулювання, особливо в умовах цифрової ери. Персональні дані містять відомості про особу, які можуть бути використані для її ідентифікації, і тому потребують особливого підходу до їхнього захисту.

В Україні захист персональних даних регулюється Законом «Про захист персональних даних», який визначає права фізичних осіб на доступ до своїх даних та контроль над їхнім використанням. Особи мають право знати, хто є розпорядником їхніх даних, з якою метою вони обробляються, а також можуть вимагати виправлення або видалення цих даних. Обробка персональних даних повинна відповідати принципам законності, прозорості, визначеності мети та мінімізації даних, що забезпечує їхнє використання виключно в законних межах.

Українське законодавство враховує міжнародні стандарти, зокрема положення Загального регламенту про захист даних ЄС (GDPR), що сприяє гармонізації правових норм і захисту прав осіб у міжнародному контексті. Особливу увагу варто приділити питанням захисту персональних даних в умовах воєнного стану, коли ризики кіберзагроз значно зростають.

Важливо зазначити, що порушення законодавства про захист персональних даних передбачає адміністративну та кримінальну відповідальність, включаючи штрафи або навіть позбавлення волі в окремих випадках. Ці положення покликані забезпечити належний рівень правового захисту і відповідальності за недобросовісне поводження з персональними даними.

Цілісний підхід до захисту персональних даних потребує дотримання норм законодавства та активного застосування сучасних технологій для захисту приватності, що є ключовим у забезпеченні безпеки особистої інформації.

Порушення права на захист персональних даних може спричинити цивільно-правову, адміністративну або кримінальну відповідальність. До цивільно-правових механізмів захисту можна віднести: вимогу про припинення неправомірного використання персональних даних, вимогу про видалення або виправлення неправдивих чи недостовірних даних, вимогу про відшкодування збитків, завданих незаконним використанням персональних даних. Особа, персональні дані якої були незаконно використані, має право вимагати відшкодування матеріальної та моральної шкоди [9]. Матеріальна шкода може містити реальні збитки, спричинені використанням персональних даних. Моральна шкода охоплює нематеріальні втрати, як-от психологічний дискомфорт або репутаційні ризики.

У нинішньому цифровому світі кіберзагрози стали серйозним викликом для безпеки особистих даних [4]. Оскільки більшість інформації зберігається в електронному вигляді, зловмисники вдаються до різних методів, щоб отримати несанкціонований доступ до конфіденційної інформації. Це створює серйозні ризики як для окремих осіб, так і для організацій.

Заключають такі типи кіберзагроз: хакерські атаки – це дії зловмисників, спрямовані на проникнення в інформаційні системи з метою викрадення, зміни або знищення даних. Фішинг – метод шахрайства, при якому зловмисники видають себе за довірених осіб або організації для отримання конфіденційної інформації, як-от логіни, паролі та фінансові дані[10].

Витоки даних – це несанкціоноване розповсюдження або продаж особистої інформації. Соціальна інженерія – маніпулятивні техніки, що використовуються для отримання доступу до конфіденційної інформації шляхом введення жертви в оману. Кіберзагрози можуть мати серйозні наслідки для приватного життя людей. Викрадення особистих даних може призвести до фінансових втрат, шахрайства, крадіжки особистості та навіть шантажу [1].

Важливо також звернути увагу на судову практику в Україні в питаннях кібербезпеки. У постанові Верховного Суду від 21.04.2021 у справі № 579/806/19 підкреслено, що особа має право відкликати згоду на обробку своїх персональних даних. Суд зазначив, що обробка персональних даних без згоди особи допускається лише у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. [8]

Перспективи розвитку правового регулювання включають гармонізацію національного законодавства з міжнародними стандартами, посилення контролю за діяльністю операторів особистих даних, а також розширення прав громадян щодо контролю над своїми даними. Одним із ключових напрямків удосконалення правового регулювання є збільшення відповідальності за порушення у сфері захисту особистих даних. Це може включати збільшення штрафів для компаній, які неправомірно використовують особисті дані, впровадження нових механізмів розслідування порушень, а також посилення ролі наглядових органів у сфері захисту особистих даних [3].

Захист особистих даних вимагає не тільки вдосконалення законодавства, а й використання інноваційних технічних рішень. Важливим є розвиток механізмів саморегулювання у сфері цифрової безпеки, що дасть змогу швидше адаптуватися до нових викликів.

Окрім правових та технічних аспектів, важливою складовою ефективного захисту особистих даних є підвищення цифрової грамотності населення. Громадяни повинні бути обізнані зі своїми правами та ризиками, пов'язаними з обробкою особистих даних. Освітні кампанії, тренінги та інтеграція теми цифрової безпеки у шкільну

та вищу освіту допоможуть формувати усвідомлене ставлення до використання особистих даних у цифровому середовищі [8].

Дослідивши проблематику можна зробити такі висновки: потреба у посиленні кібербезпеки – збільшення кількості кібератак та удосконалення тактик змушує поліпшити технічний захист особистої інформації та оновити системи безпеки. Зміцнення захисту прав осіб, чиї дані обробляються – слід спростити процедури подання скарг та підвищити ефективність розгляду справ про порушення прав тих, чиї дані обробляються. Підвищення юридичної відповідальності – теперішні санкції за незаконну обробку особистої інформації недостатньо ефективні, тому необхідні суворіші заходи та дієвіші механізми їх застосування. У цілому, відчувається потреба у комплексному реформуванні правового регулювання у сфері захисту персональних даних, яке буде враховувати технічні, організаційні та юридичні аспекти [11].

ЛІТЕРАТУРА:

1. Цивільний процесуальний Кодекс України. 2008 С. 3–214
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI: станом на 18 січ. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
3. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII: станом на 18 груд.2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII: станом на 28 черв. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.1981: станом на 6 лип. 2010 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text
6. ZakonOnline. Постанова від 21.04.2021 по справі № 579/806/19 Касаційний цивільний суд | ZakonOnline – Право знати!. Аналітично-правова система ZakonOnline. URL: https://zakononline.com.ua/court-decisions/show/96501519?utm_source (дата звернення: 11.04.2025).
7. Братасюк О.Б. Захист персональних даних: українські реалії та зарубіжний досвід. Закарпатські правові читання. Право як інструмент стійкості та розвитку в умовах сучасних цивілізаційних викликів. Частина 1. 2023. URL: <https://doi.org/10.36059/978-966-397-298-5-38>

8. Брижко В.М. Сучасні основи захисту персональних даних в правових актах. Інформація і право. 2016. № 3 (18). С. 45–57.
9. Зеркаль О.В. Деякі питання захисту персональних даних. Бюлетень Міністерства юстиції України. 2012. № 1 (123). С. 5–14.
10. Кондратенко Н.М. Щодо правового регулювання захисту персональних даних. Держава та регіони. Право. 2012. № 3 (37). С. 62–66.
11. Похиленко І. Правове регулювання захисту персональних даних. Scientific works of National Aviation University. Series: Law Journal «Air and Space Law». 2023. Т. 4, № 69. С. 94–99. URL: <https://doi.org/10.18372/2307-9061.69.18322>

Рогожа Валерія Василівна,

студентка 2-го курсу факультету прокуратури та слідства (кримінальна юстиція) Національного університету «Одеська юридична академія».

Науковий керівник: к.ю.н., доц., проф. кафедри цивільного права

Калітенко О.М.

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ: ЗАХИСТ ЧИ ЗАГРОЗА?

Інтеграція штучного інтелекту в системи кібербезпеки відкриває нові можливості для ефективного захисту даних та інформаційних інфраструктур у сучасному цифровому світі, де кіберзагрози стають дедалі складнішими та більш витонченими. З огляду на зростаючу складність і динамічність кіберзагроз, традиційні методи захисту виявляються недостатньо ефективними, що зумовлює необхідність пошуку нових підходів.

Штучний інтелект (ШІ) має потенціал значно підвищити ефективність систем кібербезпеки, забезпечуючи автоматизацію процесів виявлення загроз, аналіз аномалій, прогнозування можливих атак та адаптацію захисних механізмів у режимі реального часу. Це стає можливим завдяки здатності ШІ обробляти великі масиви даних, виявляти складні закономірності та взаємозв'язки, які можуть залишитися непомітними для людини. Проте, інтеграція ШІ в кібербезпеку супроводжується низкою викликів. Основними проблемами є забезпечення точності та надійності роботи ШІ, оскільки помилкові спрацювання можуть призвести до збоїв у системі захисту або навіть спричинити помилкове блокування ле-

Резніченко Семен Васильович НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПЕРЕВЕЗЕНЬ ПАСАЖИРІВ АВТОБУСАМИ	67
Святошнюк Арина Леонідівна ЗМІСТ ЦИВІЛЬНО-ПРАВОВИХ ВІДНОСИН У МЕРЕЖІ ІНТЕРНЕТ	73
Спасова Катерина Іванівна ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ ЦИФРОВОЇ ІДЕНТИЧНОСТІ В СОЦІАЛЬНИХ МЕРЕЖАХ	75
Токарева Віра Олександрівна ДО ПИТАННЯ ВИКОРИСТАННЯ АВТОНОМНИХ СИСТЕМ У ЗБРОЙНОМУ КОНФЛІКТІ	78
Вовчок Руслан Володимирович ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ	81
Кірсанов Олексій Володимирович ВЕРИФІКАЦІЯ БАНКІВСЬКИХ КАРТ КЛІЄНТА	85
Коштура Богдан Вячеславович ШТУЧНИЙ ІНТЕЛЕКТ ЯК УЧАСНИК ЕЛЕКТРОННИХ ПРАВОЧИНІВ	87
Романовський Денис Сергійович ІТ ПРАВА ТА КІБЕРБЕЗПЕКА ЛЮДЕЙ ПОХИЛОГО ВІКУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ	91
Рябченко Вікторія Олександрівна ПРОБЛЕМИ ЗАХИСТУ НЕПОВНОЛІТНІХ ВІД ВЕРБУВАННЯ ФСБ У СОЦМЕРЕЖІ «ТЕЛЕГРАМ»	95
Балик Даша Вікторівна ОСОБЛИВОСТІ ЗДІЙСНЕННЯ ПРАВА ВЛАСНОСТІ НА ЦИФРОВІ РЕЧІ	99
Білошкурський Микола Миколайович ЦИВІЛЬНО-ПРАВОВИЙ СТАТУС ІГРОВОЇ ОНЛАЙН-РЕЧІ НА ПРИКЛАДІ СЕРВІСУ STEAM	104
Забудько Анастасія Сергіївна ОСОБЛИВОСТІ СПАДКУВАННЯ ЦИФРОВИХ АКТИВІВ	111
Костенко Олександр Сергійович АВТОРСЬКІ ПРАВА НА ОБ'ЄКТИ, СТВОРЕНІ ШТУЧНИМ ІНТЕЛЕКТОМ: ПРАВОВІ АСПЕКТИ РЕГУЛЮВАННЯ	115
Мурашева Катерина Василівна ПЕРСОНАЛЬНІ ДАНІ ТА ЇХ ЗАХИСТ: ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ В УМОВАХ КІБЕРЗАГРОЗ	119
Рогожа Валерія Василівна РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ: ЗАХИСТ ЧИ ЗАГРОЗА?	124
Фасій Анастасія Володимирівна ДО ПИТАННЯ ПРО ПРАВОВЕ РЕГУЛЮВАННЯ РЕКЛАМИ В СОЦІАЛЬНИХ МЕРЕЖАХ	128
ВИСНОВКИ	132