УДК 347.9:004.056 DOI: https://doi.org/10.32631/pb.2025.4.04

ОЛЬГА АНАТОЛІЇВНА ЯВОР,
доктор юридичних наук, професор,
Національний юридичний університет імені Ярослава Мудрого (м. Харків),
кафедра цивільно-правової політики,
права інтелектуальної власності та інновацій;
https://orcid.org/0000-0002-5461-6498,
e-mail: yaroslava2527@gmail.com;

ТЕТЯНА СЕРГІЇВНА КИРИЧЕНКО,
кандидат юридичних наук, доцент,
Харківський національний університет внутрішніх справ,
навчально-науковий інститут № 5,
кафедра цивільного права та процесу;
https://orcid.org/0000-0002-8785-0475,
e-mail: ynatavesher021@gmail.com

ЦИВІЛЬНО-ПРАВОВІ МЕХАНІЗМИ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА УПРАВЛІННЯ РИЗИКАМИ В УКРАЇНІ В КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

Статтю присвячено розгляду цивільно-правового механізму регулювання інформаційної безпеки та управління ризиками в Україні в контексті європейської інтеграції. Встановлено й охарактеризовано інформаційне суспільство та механізм взаємодії його складових. Зазначено, що інформаційне суспільство є результатом глибинних трансформацій у сферах технологій, економіки та права, які докорінно змінюють характер соціальних і правових відносин. Проаналізовано особливості правового регулювання захисту особи й управління ризиками в цифровому просторі в контексті європейської інтеграції. Досліджено актуальність і проблеми сучасних механізмів забезпечення інформаційної безпеки, зокрема в Україні, наголошено на необхідності гармонізації законодавства з міжнародними стандартами, такими як директиви Європейського Союзу та конвенції Ради Європи. Інформаційну безпеку трактовано як систему правових і технічних заходів для захисту прав та інтересів суб'єктів у цифрових відносинах, з особливим акцентом на відповідальність, відшкодування шкоди та превентивні заходи. Досліджено роль цивільно-правових інструментів у формуванні ефективної системи захисту в умовах сучасних кіберзагроз і глобалізації, що сприяє підвищенню правової культури та правової стійкості українського інформаційного простору.

Зазначено, що сучасне розуміння інформаційної безпеки в контексті цивільного права формується на стику національного законодавства, міжнародних стандартів та доктринальних підходів. Інформаційну безпеку розглянуто не лише як сферу публічного управління, а і як важливий елемент цивільно-правових відносин, що безпосередньо стосується прав фізичних і юридичних осіб. Наведено аргументи щодо необхідності вдосконалення правових механізмів з урахуванням міжнародних стандартів і практики ЄС, зокрема в галузі управління ризиками, договірної та страхової діяльності, що сприятиме підвищенню правової стійкості України. Встановлено, що інформаційна безпека стає важливим об'єктом цивільного права, а її гарантування потребує інтеграції технічних, управлінських і правових інструментів.

Запропоновано доповнити цивільне законодавство та інші нормативно-правові акти щодо цивільно-правового механізму регулювання інформаційної безпеки й управління ризиками в Україні.

Ключові слова: *цивільно-правове регулювання, механізми захисту прав, інформаційно-правові відносини, кіберзагрози, міжнародні стандарти кіберзахисту, ризики інформаційної безпеки, юридична відповідальність, Європейська інтеграція.*

Оригінальна стаття

ВСТУП. Інформаційне суспільство є результатом глибинних трансформацій у сферах технологій, економіки та права, які докорінно змінюють характер соціальних і правових відносин. В Україні, в контексті європейської інтеграції, інтенсивне впровадження цифрових

технологій у всі сфери життя зумовлює необхідність переосмислення правових механізмів захисту особи та суспільства від нових загроз. Однією з найбільш вразливих сфер сучасності стала інформаційна безпека, яка нерозривно пов'язана з ризиками, породженими розвитком інформаційного простору. Тому цивільно-правове осмислення проблем забезпечення інформаційної безпеки та управління ризиками постає вкрай важливим завданням сучасної науки.

Цивільне право традиційно спрямоване на регулювання майнових і особистих немайнових відносин, що виникають між рівноправними суб'єктами. У цифрову епоху ці відносини зазнають якісних змін: з'являються нові об'єкти права (цифрові дані, віртуальні активи, електронні сервіси), нові ризики (несанкціонований доступ, кібератаки, інформаційний саботаж), нові способи відшкодування шкоди (страхування кіберризиків, договірні моделі управління інформаційною безпекою). Отже, виникає потреба в розробленні системи цивільно-правових механізмів, які забезпечуватимуть баланс між свободою інформаційної діяльності та належним рівнем захисту від загроз у контексті європейської інтеграції України, коли формуються нові стандарти цифрової стійкості та правової відповідальності.

Проблематика інформаційної безпеки здебільшого розглядається у площині публічного права – кримінального, адміністративного чи інформаційного. Таке домінування зумовлене тим, що держава виступає основним гарантом безпеки, реагуючи на загрози через інститути примусу та регуляторні механізми. Водночас цивільно-правовий вимір лишається менш дослідженим, хоча саме в його межах формується інструментарій відновлення порушених прав приватних осіб, компенсації матеріальних і немайнових збитків, регулювання договірних відносин у сфері цифрових послуг та запровадження превентивних засобів правового впливу.

Актуальність проблеми посилюється й тим, що інформаційна безпека має транснаціональний характер. Кіберзагрози не знають державних кордонів, що ускладнює механізми притягнення до відповідальності, визначення юрисдикції та застосування національних правових норм. Саме тому в центрі уваги цивілістичної науки опиняється завдання гармонізації вітчизняного законодавства з міжнародними та європейськими стандартами в контексті європейської інтеграції України. Практика Європейського суду з прав людини, Будапештська конвенція про кіберзлочинність, Директива (ЄС) 2022/2555 та інші документи визначають загальний вектор розвитку правових механізмів кіберзахисту, який необхідно адаптувати до українських реалій.

Особливого значення набули кібератаки на фінансові установи, що тривали протягом 2022–2023 років. Незважаючи на певні матеріальні втрати та дестабілізацію окремих сегментів банківської інфраструктури, швидкість і результативність систем реагування унеможливили критичний колапс. Окрему увагу слід звернути на напади на вебресурси органів державної влади, що супроводжувалися DDoS-атаками і поширенням провокативних повідомлень із метою дестабілізації суспільної свідомості та підриву довіри до державних інституцій.

Такі прояви кібергібридних впливів вимагають не лише технічних заходів реагування, а й належного правового забезпечення. Саме цивільне право здатне запропонувати дієві інструменти відшкодування завданих збитків, визначення меж відповідальності суб'єктів, а також формування правових гарантій безпеки учасників цифрових відносин. Розвиток цих механізмів має ґрунтуватися на поєднанні національної практики з міжнародними стандартами та рекомендаціями, зокрема Європейського Союзу та Ради Європи.

Таким чином, кібергібридні загрози стали характерною ознакою сучасного збройного конфлікту, а їхня інтенсивність і багатокомпонентність засвідчують необхідність формування ефективних правових механізмів протидії. Це зумовлює актуальність дослідження цивільно-правових інструментів забезпечення інформаційної безпеки й управління ризиками в Україні в контексті європейської інтеграції, що має стратегічне значення для захисту національних інтересів, зміцнення правової системи України та формування нової моделі цифрової стійкості держави.

Запропоноване дослідження спрямоване на заповнення наукових та практичних прогалин у вивченні цивільно-правових аспектів забезпечення інформаційної безпеки й управління ризиками. Його результати можуть стати підґрунтям для подальшої кодифікації відповідних правових норм, удосконалення судової практики та розвитку договірних інструментів, що забезпечать ефективний захист прав і свобод особи, а також стабільність функціонування національної правової системи в умовах цифрової епохи.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. *Метою* статті є з'ясування сутності цивільно-правових механізмів забезпечення інформаційної безпеки**,** визначення їхнього місця в

системі права, а також формулювання пропозицій щодо вдосконалення законодавства України в цій сфері в контексті євроінтеграційних процесів.

Досягнення поставленої мети передбачає вирішення таких *завдань*:

– проаналізувати сучасні підходи до розуміння інформаційної безпеки в контексті цивільного права;

– визначити основні ризики, що виникають в інформаційному просторі, та шляхи їх правового врегулювання;

– дослідити цивільно-правові засоби відшкодування шкоди, завданої кіберінцидентами;

– окреслити правові засади формування системи управління інформаційними ризиками та визначити роль цивільно-правових інструментів у мінімізації їх наслідків;

– обґрунтувати доцільність упровадження нових механізмів договірного та страхового регулювання кіберризиків;

– сформулювати рекомендації щодо адаптації українського законодавства до європейських і міжнародних стандартів у сфері інформаційної безпеки й управління ризиками в умовах євроінтеграції.

ОГЛЯД ЛІТЕРАТУРИ. У сучасній юридичній науковій літературі багато уваги приділяється публічно-правовим аспектам інформаційної безпеки – кримінально-правовій відповідальності, адміністративним запобіжним заходам, регуляторним стандартам. Проте приватноправовий (цивільно-правовий) підхід до проблеми є менш розвиненим.

Так, у монографії А. Ю. Нашинець-Наумової (2017) «*Інформаційна безпека: питання правового регулювання»* висвітлюються загальнонаукові та правові підходи, але акцент робиться на державному і регуляторному аспектах. Учена розглядає окремі аспекти інформаційної безпеки, зокрема у площині захисту інсайдерської інформації в корпоративному секторі. Вона приділяє увагу ризикам витоку комерційно важливих відомостей та пропонує загальні підходи до їх правового врегулювання, однак аналіз здебільшого обмежується публічно-правовими заходами, без належного висвітлення потенціалу цивільно-правових механізмів.

Подібна тенденція простежується й у статті С. П. Садковського (2023) «Деякі аспекти нормативно-правового забезпечення інформаційних технологій в контексті інформаційної безпеки України», де вчений систематизує чинні нормативно-правові акти у сфері інформаційних технологій та безпеки. Проте акцент робиться переважно на законодавчо-регулятивних положеннях та їх відповідності міжнародним стандартам, тоді як проблематика застосування цивільно-правових інструментів для захисту прав суб'єктів інформаційних відносин залишається практично поза увагою. Такий підхід демонструє наявність суттєвої наукової прогалини, адже саме приватноправові засоби здатні забезпечити відшкодування шкоди, компенсацію немайнових втрат і превентивний захист у цифровому середовищі. У роботі також здійснено системний аналіз чинних нормативно-правових актів, що регулюють сферу інформаційних технологій та кібербезпеки. Науковець розглядає національні та міжнародні документи, які визначають основні стандарти захисту інформаційних ресурсів, акцентуючи увагу на їх узгодженості із загальнодержавними стратегіями та європейськими підходами. Водночас дослідження зосереджується переважно на нормативно-регулятивному вимірі проблеми, приділяючи недостатньо уваги цивільно-правовим інструментам, що могли б забезпечити ефективний захист прав суб'єктів інформаційних відносин у разі порушення. Зокрема, поза аналізом залишаються питання відшкодування шкоди, договірного врегулювання та страхування кіберризиків. Це свідчить про те, що наявні наукові напрацювання переважно характеризують публічно-правову площину інформаційної безпеки, тоді як приватноправовий аспект лишається недостатньо дослідженим і потребує комплексного осмислення. Ці дослідження окреслюють основу, але не заповнюють прогалину в розробленні цивільно-правового інструментарію.

Дисертація І. І. Недохлєбова (2024) ґрунтується на ідеї, що інформаційна безпека є складовою національної безпеки, а її ефективне забезпечення потребує комплексного організаційно-правового механізму. Дисертант доводить необхідність гармонізації українського законодавства з європейськими стандартами, зокрема положеннями Директиви ЄС 2016/1148 (NIS Directive) та Регламенту (ЄС) 2019/881 (Cybersecurity Act). Водночас у роботі значну увагу приділено державному управлінню ризиками у сфері кіберзахисту, створенню системи національного моніторингу загроз і посиленню міжвідомчої координації. Науковець зазначає, що в Україні домінує публічно-правова модель забезпечення інформаційної безпеки, що зосереджується на інституційних і технічних аспектах, залишаючи поза належним регулюванням приватноправові відносини, пов'язані із захистом інформаційних прав суб'єктів.

У контексті нашого дослідження навчально-методичний посібник Б. А. Кормича, О. П. Федотова і Т. В. Аверочкіної (2018) «Правове регулювання інформаційної діяльності» відіграє важливу методологічну роль. У ньому сформовано концептуальне розуміння інформаційних відносин як особливого різновиду цивільних правовідносин, у межах яких реалізуються як майнові, так і немайнові права. Автори виокремлюють інститут інформаційних договорів (ліцензійних, технологічних, конфіденційності, надання інформаційних послуг), наголошуючи на потребі їх цивілістичної уніфікації відповідно до *acquis communautaire* ЄС. Вони аналізують положення законів України «Про інформацію», «Про захист персональних даних», «Про електронні документи та електронний документообіг» у взаємозв'язку із Цивільним кодексом України (далі – ЦК України), демонструючи тенденцію переходу від декларативного до договірного забезпечення інформаційної безпеки.

Дисертаційне дослідження І. М. Дороніна (2020) є однією з найбільш системних спроб осмислення правової природи національної безпеки в умовах цифрової трансформації суспільства. У центрі наукового пошуку науковця – формування комплексної моделі правового регулювання суспільних відносин, що виникають у сфері національної безпеки, з урахуванням інформаційних, технологічних і глобалізаційних чинників. Робота виконана на межі конституційного, адміністративного й інформаційного права, проте її висновки мають значну цінність і для цивілістичної доктрини, особливо в частині гарантування прав особи та управління ризиками в цифровому середовищі.

Дослідник розглядає національну безпеку як поліцентричну систему, в межах якої інформаційна безпека виступає не лише як технічна чи організаційна категорія, а і як правова цінність, безпосередньо пов'язана з реалізацією конституційних прав людини – права на інформацію, приватність, гідність і безпеку. Відповідно, одним із ключових висновків дослідника є теза про те, що в сучасну інформаційну епоху гарантії національної безпеки повинні ґрунтуватися на поєднанні публічно-правових і приватноправових засобів регулювання, де держава виконує роль координатора, а не монополіста безпеки.

Значну увагу приділено аналізу нормативно-правових актів, зокрема Конституції України, законам України «Про основи національної безпеки України» (2003) та «Про основні засади забезпечення кібербезпеки України» (2017), а також міжнародних документів – Стратегії кібербезпеки ЄС, Будапештської конвенції про кіберзлочинність (2001), Регламенту (ЄС) 2016/679 (GDPR) і Директиви ЄС 2016/1148. Дослідник доводить, що українська модель безпеки ще не досягла узгодженості з європейськими підходами насамперед через фрагментарність законодавства та слабкість механізмів цивільно-правового захисту.

У теоретичному плані І. М. Доронін уводить поняття **п**равової екосистеми національної безпеки, в якій взаємодіють державні інституції, приватні оператори критичної інфраструктури, громадянське суспільство й індивіди як носії інформаційних прав. Така екосистема передбачає управління ризиками не лише через адміністративні приписи, а й через договірні та деліктні конструкції, властиві цивільному праву: страхування кіберризиків, відшкодування шкоди, завданої витоком персональних даних, та превентивні угоди про конфіденційність. Учений акцентує, що в цифрову добу держава вже не може забезпечити повний контроль над інформаційним простором, а тому мусить створювати умови для саморегулювання і розподілу відповідальності між суб'єктами правовідносин.

Важливим внеском науковця є спроба осмислити інформаційні ризики як правову категорію. Він пропонує визначати їх як імовірність завдання шкоди об'єктам національної безпеки внаслідок протиправного використання інформаційних технологій. Дослідник наголошує на потребі нормативного закріплення принципів управління ризиками, зокрема принципів пропорційності, обґрунтованості та превентивності, які мають бути інтегровані в цивільно-правові відносини. Це положення узгоджується з європейськими підходами, закріпленими в Регламенті (ЄС) 2016/679 і Директиві (ЄС) 2022/2555, що підкреслює євроінтеграційний вектор дослідження.

Із точки зору методології І. М. Доронін застосовує системно-структурний і аксіологічний підходи, доводячи, що безпека – це не лише стан захищеності, а і процес постійного балансування прав і обов'язків у цифровому суспільстві. Його аргументація логічно веде до висновку про необхідність цивілізаційного оновлення правових гарантій – від домінування державного контролю до партнерської моделі співвідповідальності суб'єктів.

Для теми нашого дослідження робота І. М. Дороніна є особливо цінною, оскільки формує міст між національною безпекою та приватним правом. Хоча дисертація переважно зосереджена на публічно-правових інструментах,

у ній чітко простежується тенденція до визнання приватного сектору ключовим учасником системи кіберзахисту. Це відкриває простір для подальшого розвитку цивільно-правової доктрини безпеки, в межах якої правовий ризик розглядається як предмет управління, а не лише як наслідок порушення.

Узагальнюючи, можна стверджувати, що дисертація І. М. Дороніна створює ґрунтовну теоретико-правову основу для побудови сучасної системи інформаційної безпеки, орієнтованої на людиноцентризм, партнерство держави і бізнесу, дотримання європейських стандартів ризик-менеджменту та правового захисту особи. Її положення цілком можуть бути використані як методологічна база для формування цивільно-правових гарантій безпеки в інформаційному просторі та подальшої імплементації концепції «цифрового обмежувального припису» або «договірного забезпечення безпеки» в українське право.

У сучасній зарубіжній науковій доктрині поширеним є підхід, згідно з яким приватна інформація та персональні дані визнаються об'єктами цивільно-правової охорони. Такий підхід ґрунтується на розумінні інформації як нематеріального блага, що має самостійну цінність для особи та може виступати підставою для виникнення цивільних правовідносин. У наукових роботах акцентується на тому, що включення персональних даних до сфери цивільно-правового захисту забезпечує більш гнучкі механізми відновлення порушених прав, зокрема через відшкодування матеріальної та немайнової шкоди, застосування превентивних заходів і договірних конструкцій у сфері обігу інформації.

У статті Ц. Сю (2025) «*Дослідження цивільно-правового захисту приватної інформації*» здійснено порівняльний аналіз підходів різних правових систем до закріплення права на приватну інформацію в цивільних кодексах різних держав. Наголошується, що в низці країн приватна інформація визнається окремим об'єктом цивільних прав, що зумовлює можливість застосування специфічних механізмів її захисту. Серед таких механізмів виокремлюють право вимагати припинення неправомірного використання інформації, відшкодування шкоди, завданої внаслідок її незаконного поширення, а також право на компенсацію моральних втрат. Аналізуючи нормативні моделі, дослідник підкреслює значення уніфікації підходів у цій сфері та необхідність узгодження національних положень із міжнародними стандартами, що сприятиме підвищенню ефективності цивільно-правового захисту особи в цифровому середовищі. Ця робота дає корисні концептуальні підвалини для формулювання цивільно-правового підходу до кіберризиків, особливо щодо шкоди, конфіденційності та прав особи.

Деякі дослідники акцентують увагу на необхідності інтеграції кіберправа із традиційними інститутами приватного права. Зокрема, у статті У. Абдурахмана (2023) *«Взаємозв'язок кіберзаконодавства із цивільним правом: теоретичні та практичні дослідження»* обґрунтовується, що норми, спрямовані на регламентацію відносин у сфері кібербезпеки, не можуть функціонувати ізольовано від цивільного права, оскільки більшість кіберінцидентів безпосередньо зачіпають майнові та особисті немайнові права осіб. Науковець аналізує як теоретичні засади, так і практичні аспекти взаємозв'язку, наголошуючи, що ефективний захист прав в інформаційному просторі вимагає гармонізації спеціального законодавства про кібербезпеку з положеннями цивільного законодавства щодо відшкодування шкоди, укладення договорів та забезпечення відповідальності за невиконання зобов'язань. Таким чином, ми бачимо важливість комплексного підходу, в якому кіберправо розглядається не як самостійна, а як інтегрована із цивільним правом сфера, здатна забезпечити дієвий механізм захисту прав учасників інформаційних відносин.

У статті П. К. Єнг, М. А. Фаузі, Л. Сун і Б. Ян (2022) «*Оцінка правових аспектів вимог до інформаційної безпеки в галузі охорони здоров'я у трьох країнах: огляд обсягу та розробка концептуальної основи»* аналізуються вимоги безпеки у сфері охорони здоров'я, але підходи можуть бути екстрапольовані на інші галузі.

У своєму дослідженні С. Парк (2019) робить висновок, що законодавство у сфері інформаційної безпеки нерідко виявляється малоефективним через слабку імплементацію та недостатнє застосування встановлених нормативів. Дослідник наголошує, що формальне ухвалення законів не гарантує їх реальної дії у правозастосовній практиці: відсутність дієвих механізмів контролю, низький рівень правосвідомості суб'єктів і брак ефективних процедур притягнення до відповідальності нівелюють потенціал навіть добре виписаних норм. Така ситуація призводить до того, що інформаційна безпека лишається вразливою сферою, де права учасників цифрових відносин захищаються лише частково. Він доходить висновку, що для забезпечення належного рівня захисту необхідно поєднувати нормативне регулювання з розбудовою інституційної

спроможності та створенням цивільно-правових інструментів, здатних компенсувати шкоду, завдану кіберінцидентами. Зауваження науковця щодо неефективності законодавства через слабке застосування нормативів є релевантними і для України.

Попри наявність базових законів – законів України «Про інформацію»[1], «Про основні засади забезпечення кібербезпеки України»[2], а також низки підзаконних актів, спрямованих на регламентацію діяльності у сфері захисту інформаційних систем, їх практична реалізація наштовхується на низку проблем.

По-перше, відсутні чітко визначені механізми цивільно-правової відповідальності за шкоду, завдану кіберінцидентами: більшість норм мають декларативний характер і зосереджуються на організаційних заходах.

По-друге, брак узгодженості між загальними положеннями ЦК України та спеціальними нормами у сфері кібербезпеки призводить до колізій у судовій практиці, зокрема щодо відшкодування немайнової шкоди чи визначення меж відповідальності провайдерів цифрових послуг.

По-третє, низький рівень правової культури користувачів і суб'єктів господарювання зменшує ефективність навіть тих механізмів, які формально існують.

У результаті законодавство України у сфері інформаційної безпеки нині має радше превентивно-декларативний характер, ніж компенсаторно-правозастосовний. Саме тому в українських реаліях особливо актуальною є імплементація європейських стандартів, зокрема положень Директиви (ЄС) 2022/2555 (NIS2 Directive**)**, що передбачає не лише обов'язки операторів критичної інфраструктури, а й чіткі механізми цивільно-правової відповідальності[3]. Поєднання таких норм із модернізованими положеннями ЦК України (про страхування кіберризиків, договірні зобов'язання у сфері кіберзахисту, компенсацію матеріальної та моральної шкоди від кіберінцидентів) дозволить зробити інформаційне право в Україні справді дієвим, а не лише формально закріпленим. Розглянуті вище наукові праці допомагають зрозуміти складнощі інтеграції цифрових стандартів і цивільно-правових норм.

Деякі дослідження зосереджені на вивченні галузевої специфіки інформаційної безпеки, де питання захисту інформаційних відносин набуває особливого значення. Так, у статті І. В. Поліщука (2020) «Особливості правового регулювання інформаційної безпеки в цивільній авіації України» проведено аналіз чинних нормативно-правових актів, що регулюють безпеку інформаційних систем у сфері авіаційної діяльності. Дослідник обґрунтовує, що авіаційна галузь є надзвичайно вразливою до інформаційних загроз, оскільки стабільність функціонування повітряного транспорту прямо залежить від безперебійності і захищеності інформаційних потоків. Наголошується на потребі в розробленні спеціалізованих галузевих норм, які б ураховували специфіку авіаційних перевезень, високі стандарти міжнародної авіаційної безпеки, а також інтеграцію з європейськими та міжнародними вимогами. На думку науковця, лише поєднання загальних принципів інформаційного права з галузевими стандартами дозволить створити дієву систему захисту інформаційних відносин у сфері цивільної авіації, що забезпечить як безпеку пасажирів, так і стабільність транспортної інфраструктури держави.

У статті Н. В. Сугоняко (2019) «Інформаційна безпека в інформаційній діяльності суду» розглядаються доктринальні підходи до забезпечення захищеності інформаційних систем у сфері правосуддя. Учена наголошує, що сучасні судові установи функціонують в інформаційному просторі, який потребує надійного правового і технічного регулювання, адже вразливість інформаційних ресурсів суду може підірвати принципи доступності правосуддя, конфіденційності даних та довіри громадян до судової влади. У статті акцентовано, що ключовим завданням є створення правових механізмів, які б унеможливлювали несанкціонований доступ до матеріалів справ, забезпечували захист персональних даних

---

1 Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 28.09.2025).

2 Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 28.09.2025).

3 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) // EUR-Lex : сайт. URL: http://data.europa.eu/eli/dir/2022/2555/oj (дата звернення: 28.09.2025).

учасників процесу та гарантували стабільність роботи електронних судових систем. Науковиця наголошує на необхідності узгодження національного законодавства з міжнародними стандартами, а також розроблення внутрішньогалузевих нормативних актів, які б ураховували специфіку судочинства. Таким чином, дослідження показує, що інформаційна безпека в судовій діяльності є не лише технічним, а й фундаментальним правовим інститутом, який має забезпечувати реалізацію конституційних гарантій на справедливий суд. У статті А. Ю. Нашинець-Наумової (2013) розглядається двосторонній підхід – як до інформації на об'єктах, так і до інформаційних систем, що передають дані. Ці дослідження демонструють, що в окремих секторах уже існує спроба глибшого правового осмислення, але майже завжди в межах галузі, а не загального цивільно-правового підходу.

У статті К. Дель-Реал, Е. Буссер і Б. Берг (2025) «*Систематичний огляд літератури з питань безпеки та конфіденційності за принципами, нормами та стратегіями проєктування цифрових технологій*» розглядаються принципи «безпека за замовчуванням» (*security by design*) і «конфіденційність за замовчуванням» (*privacy by design*) у цифрових системах, що мають пряме відношення до управління ризикам. У міжнародному контексті робота Ф. Контіні й А. Корделли (2017) «*Право та технології в цивільному судочинстві*» показує, як технології впливають на судовий процес, що також ставить питання про взаємозв'язок технічних систем і правового регулювання. Такі підходи важливі для методологічної бази у процесі формулювання власних моделей цивільно-правового захисту.

Українські дослідження частіше обмежуються нормативно-правовим аналізом і публічно-правовими аспектами, тоді як конкретні механізми компенсації шкоди, договірного захисту або страхування кіберризиків розкриті фрагментарно. Більшість робіт присвячені або праву, або кібербезпеці, але не об'єднують правові, технічні й економічні підходи. Це створює розрив між теорією цивільного права та практикою кіберзахисту. Лише деякі праці аналізують іноземні моделі захисту інформації (особливо в Китаї або країнах, де вже існує цивільно-правовий захист приватної інформації). Це обмежує можливості адаптації успішного досвіду. У багатьох працях використовують різні дефініції інформаційної безпеки, цифрових активів або кіберризиків, що ускладнює їх порівняння та синтез. Тому вкрай необхідне формування єдиного понятійного апарату для цивільно-правового контексту. У літературі рідко можна зустріти аналіз таких осіб, як провайдер, оператор, користувач, адміністратор, а також критерії, які визначають відповідність їхніх дій.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. Методологічну основу статті становить комплекс загальнонаукових, спеціально-юридичних і міждисциплінарних методів, які в сукупності забезпечують цілісність аналізу проблематики інформаційної безпеки, її цивільно-правового забезпечення та розвитку в контексті євроінтеграційних процесів України.

Діалектичний метод використано для з'ясування сутності категорії «інформаційна безпека» в розвитку та взаємозв'язку із цивільно-правовими інститутами. Він надав змогу виявити трансформацію правового регулювання під впливом цифровізації, глобалізації та євроінтеграції України в єдиний європейський правовий простір.

Аналіз і синтез застосовувалися для дослідження структури ризиків, виокремлення їхніх цивільно-правових аспектів і визначення напрямів гармонізації з європейськими підходами до управління інформаційними ризиками.

Індукція та дедукція сприяли формулюванню висновків щодо загальних закономірностей розвитку правових механізмів кіберзахисту на основі конкретних прикладів національної, європейської та міжнародної практики.

Системний підхід дозволив розглядати інформаційну безпеку як багаторівневий феномен, що поєднує технічний, правовий, економічний і соціальний виміри в умовах євроінтеграційного розвитку правової системи України.

Формально-юридичний метод використано для аналізу положень ЦК України, Закону України «Про основні засади забезпечення кібербезпеки України», а також міжнародних актів – Будапештської конвенції про кіберзлочинність, Директиви (ЄС) 2022/2555 та інших документів, що формують основу євроінтеграційного правового простору у сфері інформаційної безпеки.

Порівняльно-правовий метод надав змогу зіставити підходи до врегулювання цивільно-правових аспектів кіберризиків, договорів у сфері інформаційних послуг і страхування кіберзагроз в Україні та країнах Європейського Союзу, що має важливе значення для адаптації національного законодавства до *acquis communautaire* ЄС.

Метод правового моделювання застосовано для формулювання пропозицій щодо вдосконалення цивільно-правових механізмів

управління ризиками й адаптації законодавства України до європейських стандартів у межах євроінтеграційного курсу держави.

Оскільки предмет дослідження перебуває на стику права, інформаційних технологій і кібербезпеки, використовувався комплексний міжгалузевий аналіз, який дозволив інтегрувати знання з комп'ютерних наук (класифікація кіберризиків, специфіка атак), економіки (оцінка вартості збитків, страхування ризиків) і соціології (вплив інформаційних атак на суспільну довіру та правосвідомість). Застосування міждисциплінарного підходу надало можливість виявити тенденції формування правових засад інформаційної безпеки України в європейському правовому контексті.

Емпіричну базу дослідження становлять:

– законодавство України;

– міжнародні акти у сфері кібербезпеки – Будапештська конвенція про кіберзлочинність, документи Ради Європи, ЄС і НАТО;

– рішення Європейського суду з прав людини (зокрема у справах *Delfi AS v. Estonia*, *K.U. v. Finland*), що висвітлюють європейські стандарти захисту інформаційних прав і сприяють реалізації євроінтеграційного курсу України.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. Сучасне розуміння інформаційної безпеки в контексті цивільного права формується на стику національного законодавства, міжнародних стандартів і доктринальних підходів. В Україні в умовах євроінтеграції та наближення до *acquis communautaire* ЄС, а також у правовій доктрині інформаційна безпека розглядається не лише як категорія публічного права, що забезпечується державою через адміністративні і кримінально-правові інструменти, а й як елемент цивільно-правових відносин, безпосередньо пов'язаний із реалізацією та захистом суб'єктивних прав фізичних і юридичних осіб.

Таким чином, сучасні підходи до розуміння інформаційної безпеки в цивільному праві відходять від її виключно технічного чи кримінально-правового трактування і фокусуються на забезпеченні балансу між інтересами держави, бізнесу та особи. Інформаційна безпека стає об'єктом цивільних правовідносин, а її ефективний захист потребує вдосконалення національного законодавства шляхом закріплення спеціальних цивільно-правових механізмів, гармонізованих з європейськими стандартами та практикою.

Правовою основою забезпечення кібербезпеки України є: Конституція України, закони України «Про основи національної безпеки України» та «Про основні засади забезпечення кібербезпеки України» (засади внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом), Будапештська конвенція про кіберзлочинність 2001 року[1], інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що ухвалюються на виконання законів України. Зазначена система джерел розвивається з урахуванням євроінтеграційних зобов'язань України та потреби наближення до права ЄС.

Відповідно до Закону України «Про інформацію» інформаційна безпека трактується як стан захищеності інформації та інформаційних ресурсів від неправомірного впливу, що гарантує дотримання прав особи та суспільства на доступ, використання, поширення та збереження інформації[2]. Закон України «Про основні засади забезпечення кібербезпеки України» закріплює засади формування національної системи кіберзахисту та визначає її суб'єктів, серед яких є і приватні юридичні особи, що діють як оператори критичної інфраструктури[3]. Це свідчить про розширення цивільно-правового виміру інформаційної безпеки, оскільки на суб'єктів приватного права покладаються конкретні обов'язки із захисту даних та управління ризиками, узгоджені з підходами ЄС.

Згідно з положеннями ЦК України (статті 15, 16, 23, 1166) особа має право на захист своїх особистих немайнових і майнових прав у разі їх порушення, зокрема шляхом поширення неправдивої інформації, незаконного доступу до персональних даних або блокування цифрових ресурсів[4]. Таким чином, інформаційна безпека є

---

1 Конвенція про кіберзлочинність : від 23.11.2001 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 28.09.2025).

2 Про інформацію : Закон України від 02.10.1992 № 2657-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 28.09.2025).

3 Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 28.09.2025).

4 Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.

об'єктом цивільно-правового захисту, а її порушення є підставою для застосування відшкодування шкоди та інших способів цивільно-правового захисту.

Будапештська конвенція про кіберзлочинність та Директива (ЄС) 2022/2555 підкреслюють важливість поєднання державного та приватного компонентів безпеки. Вони зобов'язують держав-учасниць упроваджувати не лише кримінально-правові механізми боротьби з кіберзлочинами, а й ефективні процедури відшкодування шкоди, завданої порушенням інформаційної безпеки. У цьому аспекті особливого значення набуває розвиток договірних інструментів у сфері цифрових послуг, а також інституту страхування кіберризиків, що є превентивним засобом управління ризиками в цивільно-правовій площині відповідно до євроінтеграційного курсу України**.**

В Україні об'єктами кіберзахисту є:

1) інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) інформаційні, електронні комунікаційні й інформаційно-комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного врядування, електронних державних послуг, електронної комерції, електронного документообігу[1].

Одним із ключових напрямів забезпечення функціонування національної системи кібербезпеки є запровадження нормативно-правового регулювання у сфері кібербезпеки та кіберзахисту з урахуванням ризик-орієнтованого підходу, чіткого розподілу ролей, завдань, функцій і відповідальності серед публічного сектору, операторів критичної інфраструктури, а також власників чи розпорядників об'єктів критичної інформаційної інфраструктури. Важливою є також гармонізація із практиками і стандартами Європейського Союзу та НАТО.

Європейський Союз також переживає серйозні кіберзагрози, що підтверджується численними випадками кібератак. За даними звіту Федерального кримінального поліцейського управління Німеччини, у 2024 році в Німеччині було зареєстровано 131 391 випадок кіберзлочинів, а ще 201 877 інцидентів були здійснені з-за кордону або з невстановлених локацій. Переважна більшість атак на німецькі об'єкти, як зазначають у звіті, мала проросійське або антиізраїльське забарвлення, зокрема цілями були державні установи. Програми-вимагачі стали однією з найбільших загроз: у 2024 році 950 компаній і організацій повідомили про подібні інциденти. Німецька цифрова асоціація Bitkom підрахувала, що шкода, завдана кібератаками, досягла 178,6 млрд євро (203,87 млрд дол. США) – на 30,4 млрд євро більше, ніж у попередньому році (Гурін, 2025). Ці цифри підкреслюють необхідність Україні орієнтуватися на досвід ЄС у питаннях кіберстійкості та управління інцидентами.

У сфері кібербезпеки існує низка міжнародних стандартів, які визначають вимоги до захисту інформаційних систем, управління ризиками та забезпечення конфіденційності, цілісності та доступності даних:

– BS 7799-1:1999 «Управління інформаційною безпекою» (базовий британський стандарт) – містить коди практики управління інформаційною безпекою та управління ризиками[2];

– NIST Cybersecurity Framework – рамковий документ Національного інституту стандартів і технологій США, який визначає п'ять основних функцій: ідентифікація, захист, виявлення, реагування та відновлення; використовується для управління кіберризиками[3].

Застосування цих стандартів посилює стійкість організацій до кіберзагроз і підвищує довіру користувачів та партнерів.

Основними правовими актами, що регулюють кібербезпеку в Європейському Союзі, є, зокрема, Регламент (ЄС) 2019/881[4] та Директива

gov.ua/laws/show/435-15 (дата звернення: 28.09.2025).

1 Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 28.09.2025).

2 BS 7799-1:1999. Information security management. Part 1: Code of practice for information security management. London : BSI, 1999. 52 p.

3 Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. April 16, 2018. DOI: https://doi.org/10.6028/NIST.CSWP.04162018.

4 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity

(ЄС) 2022/2555 (NIS2 Directive)[1]. Одним із важливих нововведень є створення єдиного механізму управління інцидентами. Згідно з положеннями Директиви (ЄС) 2022/2555 держави-члени повинні запровадити чітку структуру відповідальних органів, таких як компетентні національні органи та комп'ютерні групи реагування на інциденти безпеки (*Computer Security Incident Response Team*). Взаємодія ЄС з іншими регіональними ініціативами демонструє прагнення до створення глобальної системи кібербезпеки. Співпраця з Асоціацією держав Південно-Східної Азії, НАТО, Організацією американських держав та Африканським Союзом дозволяє обмінюватися кращими практиками та підвищувати рівень готовності до кіберзагроз (Зінченко, 2024). Для України це є важливими орієнтирами в межах євроінтеграційної траєкторії.

Для координації та підвищення ефективності заходів у сфері кіберзахисту на рівні Європейського Союзу функціонує Європейське агентство з кібербезпеки *(European Union Agency for Cybersecurity*, далі – ENISA)**,** діяльність якого спрямована на розроблення стандартів, проведення спеціалізованих навчань і сприяння у впровадженні нормативних актів, зокрема Директиви (ЄС) 2016/1148 та Директиви (ЄС) 2022/2555. Інституційна роль ENISA полягає не лише у формуванні загальноєвропейських стандартів кіберстійкості, але й у створенні умов для гармонізації національних систем реагування на кіберзагрози держав – членів ЄС[2].

В Україні національна система реагування на кіберінциденти охоплює низку інституційних суб'єктів, що взаємодіють у межах єдиної архітектури кібербезпеки. Ключове місце серед них посідає CERT-UA – національна команда реагування на комп'ютерні інциденти, створена на підставі Закону України *«Про основні засади забезпечення кібербезпеки України»*. Вона координує заходи з виявлення, запобігання та усунення наслідків кібератак. Важливу роль також відіграють галузеві та регіональні команди реагування на комп'ютерні інциденти, діяльність яких визначається відповідними підзаконними актами і відомчими нормативними документами. До системи державних органів, що протидіють кіберзагрозам, залучаються Національна поліція України та Служба безпеки України. Їхня компетенція у сфері інформаційної безпеки регламентується законами України *«Про Національну поліцію»*[3] та *«Про Службу безпеки України»*[4]. Окрім цього, у структурі національної кібербезпеки діють приватні команди реагування, що забезпечують захист корпоративних інформаційних систем і взаємодіють із державними інституціями в разі масштабних інцидентів, що відповідає підходам, закріпленим у Стратегії кібербезпеки України[5].

Вищий рівень стратегічної координації забезпечує Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України, який визначає пріоритети державної політики у сфері кіберзахисту, координує діяльність суб'єктів сектору безпеки та оборони і забезпечує узгодженість заходів із міжнародними партнерами.

Таким чином, національна модель кібербезпеки України функціонує як багаторівнева система, що інтегрує діяльність державних органів, галузевих структур та приватних інституцій, забезпечуючи комплексний підхід до протидії кіберзагрозам і поступово наближаючи її до європейських практик, визначених, зокрема, у Директиві (ЄС) 2022/2555. Відповідні засади закріплено в Законі України «Про основні засади забезпечення кібербезпеки України»**.**

certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) // EUR-Lex : сайт. URL: http://data.europa.eu/eli/reg/2019/881/oj (дата звернення: 28.09.2025).

1 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) // EUR-Lex : сайт. URL: http://data.europa.eu/eli/dir/2022/2555/oj (дата звернення: 28.09.2025).

2 What we do // European Union Agency for Cybersecurity :офіц. сайт. URL: https://www.enisa.europa.eu/about-enisa/what-we-do (дата звернення: 28.09.2025).

3 Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 28.09.2025).

4 Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 28.09.2025).

5 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 28.09.2025).

У науковій літературі наголошується, що ефективність управління ризиками у сфері кібербезпеки значною мірою залежить від використання системних методологій. Так, П. Г. Сидоркін, С. О. Горліченко, В. С. Некоз і М. В. Шилан (2023) зазначають, що ключовим елементом аналізу й управління ризиками відповідно до моделі «Контрольні цілі для інформаційних та суміжних технологій» (*Control Objectives for Information and Related Technology*, далі – COBIT) є формування ризикових сценаріїв. Для кожного такого сценарію визначається його належність до певного типу ризику: стратегічні ризики, що стосуються втрачених можливостей використання інформаційних технологій для розвитку та підвищення ефективності діяльності організації; проєктні ризики, пов'язані зі впливом інформаційних технологій на створення чи модернізацію внутрішніх процесів; ризики управління інформаційними технологіями та надання IT-сервісів, які охоплюють проблеми забезпечення їх доступності, стабільності та якості. Імплементація таких рамок корелює з європейською практикою управління кіберризиками.

Кожен ризиковий сценарій у межах зазначеного підходу включає кілька ключових характеристик: джерело загрози (внутрішнє чи зовнішнє), її тип (зловмисна дія, техногенна чи природна подія, помилка), опис події (несанкціонований доступ, знищення або зміна даних, розкриття інформації, крадіжка), перелік активів організації, на які може впливати загроза (персонал, бізнес-процеси, IT-інфраструктура), а також часові межі події. Подальший аналіз передбачає оцінювання відповідності виявлених ризиків до ризик-апетиту організації та ухвалення одного з рішень: уникнення ризику, його прийняття, передачі (через договори або страхування) чи зниження за допомогою превентивних заходів.

Таким чином, упровадження ризик-орієнтованого підходу, заснованого на міжнародних моделях, таких як COBIT, дозволяє інтегрувати технічні й управлінські рішення у правові механізми забезпечення кібербезпеки. Це сприяє формуванню більш гнучкої та адаптивної системи цивільно-правового захисту, здатної адекватно реагувати на сучасні цифрові виклики.

Інформаційна безпека у країнах Європи стикається з низкою суттєвих викликів, одним з яких є недостатня узгодженість політик на рівні Європейського Союзу. Це ускладнює ефективну співпрацю між державними органами та приватним сектором і створює перепони для впровадження загальноєвропейських стандартів захисту критичної інформаційної інфраструктури. Серед основних кіберзагроз у європейських країнах – організована кіберзлочинність, включаючи шахрайські дії, цілеспрямовані хакерські атаки, поширення забороненого контенту, а також масовані DDoS-атаки, що призводять до збою роботи електронних комунікаційних систем[1]. Особливу увагу в Європі приділяють захисту персональних даних відповідно до вимог Регламенту (ЄС) 2016/679[2] та інших директив ЄС.

Проте рівень розвитку інфраструктури кібербезпеки та здатність до оперативного реагування значно варіюються серед країн-членів, що підкреслює необхідність посилення міждержавної координації.

Забезпечення інформаційної безпеки в Європі є багаторівневим і комплексним процесом, який потребує поглиблення міжнародної співпраці, уніфікації нормативних підходів та ефективного партнерства між державним і приватним секторами для протидії постійно зростаючим кіберзагрозам. Для України гармонізація із цими підходами є важливою складовою євроінтеграційної стратегії.

В Україні основні ризики інформаційної безпеки зосереджені на кіберзагрозах, що спрямовані насамперед на об'єкти критичної інфраструктури, зокрема в галузях енергетики і транспорту. Вразливість цих систем зумовлена як технічними, так і організаційними проблемами, що існують у національній системі кібербезпеки. Загрози значно посилилися на тлі російської агресії, де інформаційні технології відіграють ключову роль у гібридній війні.

Інформаційний простір, який сьогодні охоплює всі сфери суспільного життя – від комунікацій до фінансових транзакцій, породжує широкий спектр ризиків, що безпосередньо впливають на реалізацію і захист цивільних прав. До найбільш поширених ризиків можна віднести: по-перше, несанкціонований доступ

---

1 ENISA Threat Landscape 2022 (July 2021 to July 2022). October 2022 // ENISA : офіц. сайт. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (дата звернення: 28.09.2025).

2 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, and repealing Directive 95/46/EC (General Data Protection Regulation) // EUR-Lex : сайт. URL: http://data.europa.eu/eli/reg/2016/679/oj (дата звернення: 28.09.2025).

до персональних даних та комерційної таємниці, що порушує право на приватність і власність на інформаційні ресурси; по-друге, порушення конфіденційності і цілісності електронних транзакцій, що ставить під загрозу стабільність договірних відносин у сфері електронної комерції; по-третє, поширення недостовірної інформації, яке може завдати шкоди честі, гідності і діловій репутації особи; почетверте, блокування або дестабілізація роботи інформаційних систем і цифрових платформ, що спричиняє матеріальні збитки і упущену вигоду; по-п'яте, репутаційні ризики, пов'язані з кібератаками на суб'єктів господарювання, які можуть призвести до втрати клієнтів та партнерів.

Шляхи правового врегулювання ризиків у цивільно-правовій площині передбачають як компенсаційні, так і превентивні механізми. Згідно зі статтями 16, 22, 23 та 1166 Цивільного кодексу України особа, якій завдано шкоди внаслідок порушення інформаційної безпеки, має право на відшкодування реальних збитків, упущеної вигоди та моральної шкоди[1]. Цей підхід відповідає європейськими стандартами ефективного правового захисту.

Таке регулювання дає підстави кваліфікувати кіберінциденти як підставу для цивільно-правової відповідальності. Водночас Закон України «Про основні засади забезпечення кібербезпеки України» встановлює обов'язки суб'єктів критичної інфраструктури щодо впровадження систем захисту, що в перспективі повинно отримати подальшу деталізацію в цивільному законодавстві шляхом розроблення спеціальних договірних моделей для надання послуг із кіберзахисту.

Важливим інструментом зниження ризиків є страхування кіберризиків, що вже активно застосовується в європейських країнах відповідно до Директиви (ЄС) 2022/2555. Для України актуальним є закріплення в ЦК України спеціальних положень, що регулюють можливість укладення договорів страхування кіберризиків як окремого виду майнового страхування. Крім того, необхідним є розвиток судової практики у сфері захисту немайнових прав у цифровому середовищі з урахуванням прецедентів Європейського суду з прав людини, зокрема у справах *Delfi AS v. Estonia*[2] та *K.U. v. Finland*[3], у яких сформульовано стандарти відповідальності за порушення інформаційних прав.

Отже, правове врегулювання ризиків цифрового середовища має здійснюватися на трьох рівнях: через удосконалення цивільно-правових механізмів відшкодування шкоди, розширення договірних і страхових інструментів управління ризиками, а також через гармонізацію національного законодавства з міжнародними стандартами у сфері кіберзахисту. Це дозволить не лише ефективно захищати права осіб, а й значно підвищити рівень цифрової стійкості держави.

У сучасному інформаційному просторі кіберінциденти вже не є лише технічною, але й серйозною правовою проблемою, оскільки їх наслідки безпосередньо впливають на реалізацію цивільних прав і породжують обов'язок відшкодування завданої шкоди. Цивільне право забезпечує найбільш гнучкі механізми відновлення порушених прав, поєднуючи компенсаційні та превентивні засоби.

Основним універсальним інструментом є відшкодування майнової шкоди. Відповідно до ст. 1166 ЦК України шкода, завдана неправомірними діями, підлягає відшкодуванню в повному обсязі[4]. Це положення охоплює як прямі втрати (знищення чи блокування цифрових ресурсів, пошкодження обладнання), так і упущену вигоду, що може виникати внаслідок зупинки бізнес-процесів або переривання електронних транзакцій.

Окреме значення має відшкодування моральної (немайнової) шкоди, передбачене ст. 23 ЦК України[5]. У разі кіберінцидентів така шкода може полягати у приниженні честі, гідності чи ділової репутації особи, зокрема через поширення неправдивих даних, незаконний доступ до персональної інформації або її

---

1 Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 28.09.2025).

2 Справа «Delfi AS проти Естонії» (Заява № 64569/09) : рішення Європейського суду з прав людини від 16.06.2015 // HUDOC : сайт. URL: https://hudoc.echr.coe.int/eng?i=001-163044 (дата звернення: 28.09.2025).

3 Справа «K.U. v. Finland» (Заява № 2872/02) : рішення Європейського суду з прав людини від 02.03.2009 // HUDOC : сайт. URL: https://hudoc.echr.coe.int/eng?i=001-117605 (дата звернення: 28.09.2025).

4 Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 28.09.2025).

5 Там само.

публікацію без згоди власника. Ураховуючи прецеденти Європейського суду з прав людини, зокрема у справах *Delfi AS v. Estonia* та *K.U. v. Finland*, національна судова практика повинна визнавати, що цифровий простір не є зоною безвідповідальності, а порушення інформаційних прав обов'язково повинно супроводжуватися відшкодуванням немайнових втрат.

Ефективним інструментом для відновлення порушених прав може бути визнання інформації недостовірною та її спростування (ст. 277 ЦК України)[1]. Цей спосіб захисту особливо актуальний у разі поширення неправдивої інформації в соціальних мережах чи інших цифрових каналах комунікації, коли матеріальні збитки важко обчислити, але є потреба у відновленні репутації та довіри.

Розвиток договірних і страхових механізмів знижує навантаження на суди, стимулює впровадження сучасних стандартів безпеки як умови страхового покриття та гармонізує українське право з вимогами ЄС (зокрема з Директивою (ЄС) 2022/2555). Це підвищує рівень захисту прав учасників інформаційних відносин і сприяє зміцненню стійкості України.

Перспективним напрямом є розвиток договірних конструкцій у сфері інформаційних послуг. Включення спеціальних умов щодо відповідальності за кіберінциденти в договори із провайдерами, операторами інформаційних систем чи постачальниками хмарних сервісів дозволить забезпечити додаткові гарантії для користувачів. Аналогічно може застосовуватися страхування кіберризиків як превентивний засіб управління ризиками: в разі настання інциденту страховик відшкодовує завдані збитки, що підвищує рівень захищеності суб'єктів цифрових відносин.

Таким чином, цивільно-правові засоби відшкодування шкоди від кіберінцидентів охоплюють як традиційні інструменти (відшкодування матеріальних і немайнових збитків, визнання та спростування недостовірної інформації), так і нові превентивні форми, зокрема договірне регулювання та страхування кіберризиків. Подальший розвиток цих засобів має ґрунтуватися на гармонізації національного права з європейськими стандартами та формуванні сталої судової практики у сфері цифрової безпеки.

Розвиток цифрової економіки і трансформація інформаційних відносин зумовили появу нових видів ризиків, які неможливо нейтралізувати виключно технічними чи адміністративними засобами. Кіберінциденти завдають шкоди не лише державі, а й безпосередньо приватним суб'єктам – фізичним та юридичним особам, що укладають договори, здійснюють фінансові транзакції або користуються інформаційними послугами. Отже, традиційні механізми цивільно-правової відповідальності потребують доповнення інноваційними засобами управління ризиками, серед яких особливе значення мають договірні та страхові інструменти.

Договірне регулювання кіберризиків дозволяє сторонам заздалегідь визначити обсяг відповідальності, порядок дій у разі кіберінциденту і механізми компенсації збитків. Укладання договорів із провайдерами інформаційних послуг, постачальниками програмного забезпечення чи операторами хмарних сервісів може включати умови щодо: обов'язку впровадження стандартів безпеки, повідомлення про інциденти, порядку відшкодування збитків і меж відповідальності. Це відповідає принципу свободи договору (ст. 6 ЦК України[2]) та водночас створює передумови для зниження невизначеності у правовідносинах.

Страхування кіберризиків є превентивним інструментом, що забезпечує фінансову стабільність у випадках, коли встановлення конкретного винуватця або стягнення з нього збитків є ускладненим. У світовій практиці страхові компанії покривають витрати на відновлення даних, компенсацію клієнтам, судові витрати, пов'язані з витоком інформації, або репутаційні втрати. Для України актуальним є доповнення положень ЦК України про майнове страхування (статті 979–999) спеціальною нормою щодо можливості укладення договорів страхування кіберризиків. Це сприятиме розвитку відповідного ринку та формуванню комплексної системи захисту прав осіб у цифровому середовищі.

Упровадження таких механізмів має низку переваг: по-перше, воно знижує навантаження на судову систему, оскільки частина спорів вирішується превентивно на підставі договорів чи страхових виплат; по-друге, стимулює суб'єктів господарювання впроваджувати

1 Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 28.09.2025).

2 Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 28.09.2025).

сучасні стандарти інформаційної безпеки, що є умовою страхового покриття; по-третє, гармонізує національне законодавство з європейськими стандартами, зокрема з положеннями Директиви (ЄС) 2022/2555, яка передбачає обов'язок управління ризиками та відповідальність операторів критичної інфраструктури.

Таким чином, упровадження нових договірних і страхових механізмів у сфері цивільного права є доцільним та необхідним кроком, який дозволить підвищити рівень захисту прав осіб від кіберзагроз, забезпечити баланс інтересів між користувачами, постачальниками послуг і державою, а також сприятиме зміцненню цифрової стійкості України.

Важливою проблемою залишається недостатній рівень координації між відповідальними структурами, а також неповне нормативно-правове регулювання і технічне недосконале забезпечення. Людський фактор також суттєво впливає на стан безпеки: нестача кваліфікованих фахівців, високий рівень плинності персоналу, а також прогалини у впровадженні сучасних процедур, таких як резервне копіювання інформації та двофакторна автентифікація.

Усі ці аспекти обмежують ефективність національної політики кіберзахисту, створюючи умови для виникнення інцидентів, що можуть негативно позначитися не лише на безпеці України, а й на стабільному функціонуванні критичної інфраструктури та державних систем. Тому для подолання цих викликів необхідне комплексне та системне оновлення підходів до захисту інформаційних систем критичної інфраструктури відповідно до європейських стандартів і в контексті євроінтеграції України.

ВИСНОВКИ. Інформаційна безпека набуває ознак самостійного об'єкта цивільно-правового регулювання, оскільки стосується охорони майнових та особистих немайнових прав осіб у сфері інформаційних відносин. Кібергібридні загрози мають транснаціональний і багаторівневий характер, що вимагає комплексного поєднання технічних, організаційних і правових засобів. Чинне законодавство України, зокрема Цивільний кодекс України, законодавство про інформацію, кібербезпеку, захист персональних даних, містить лише фрагментарні положення щодо управління ризиками, не формуючи цілісної системи цивільно-правових механізмів.

Цивільно-правові засоби захисту прав у сфері інформаційної безпеки повинні виконувати як компенсаційну (відшкодування шкоди), так і превентивну (страхування ризиків, договори кіберзахисту) функції. Актуальною є проблема визначення меж цивільної відповідальності суб'єктів, які надають цифрові послуги, обробляють персональні дані або управляють критичною інформаційною інфраструктурою.

В умовах євроінтеграції України пріоритетним стає наближення приватноправових механізмів до стандартів ЄС, зокрема щодо управління ризиками, відповідальності постачальників послуг та ефективних засобів правового захисту.

Ураховуючи вищевикладене, пропонуємо внести відповідні зміни до чинного законодавства України.

1. Цивільний кодекс України: доповнити окремою главою про *цивільно-правовий захист прав в інформаційних відносинах*, де визначити поняття «інформаційна безпека» як об'єкт цивільних прав; уточнити норми про відшкодування шкоди, завданої інформаційними діями (кібератаками, неправомірним поширенням даних, блокуванням доступу до інформаційних ресурсів та систем) з урахуванням *acquis communautaire* ЄС щодо ефективних засобів захисту.

2. У Законі України «Про основні засади забезпечення кібербезпеки України» розширити положення щодо цивільно-правової відповідальності операторів критичної інфраструктури; запровадити норми про обов'язкове страхування кіберризиків для суб'єктів, діяльність яких пов'язана з обробкою великих масивів персональних даних чи фінансових транзакцій, у логіці імплементації Директиви (ЄС) 2022/2555 та європейських практик управління інцидентами.

3. Імплементувати в національне право положення Директиви (ЄС) 2022/2555 і Будапештської конвенції про кіберзлочинність з акцентом на приватноправові гарантії захисту; закріпити механізми міжнародного співробітництва у сфері відшкодування шкоди, завданої кіберзлочинами.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Гурін А. У Німеччині заявили про рекордний рівень кіберзлочинності через атаки проросійських та антиізраїльських хакерів // ZN,UA : сайт. 03.06.2025. URL: https://zn.ua/ukr/europe/u-nimechchini-zajavili-pro-rekordnij-riven-kiberzlochinnosti-cherez-ataki-prorosijskikh-ta-antiizrajilskikh-khakeriv.html (дата звернення: 28.09.2025).

2. Доронін І. М. Правове регулювання суспільних відносин у сфері національної безпеки в інформаційну епоху : дис. … д-ра юрид. наук : 12.00.01. Київ, 2020. 458 с.

3. Зінченко О. І. Європейські регіональні засоби протидії кібертероризму. *Регіональні студії.* 2024. № 39. С. 94–100. DOI: https://doi.org/10.32782/2663-6170/2024.39.15.

4. Кормич Б. А., Федотов О. П., Аверочкіна Т. В. *Правове регулювання інформаційної діяльності* : навч.-метод. посіб. Одеса : Нац. ун-т «Одеська юридична академія», 2018. 156 с.

5. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с.

6. Нашинець-Наумова А. Ю. Правове регулювання інформаційної безпеки в цивільній авіації: міжнародно-правовий аспект. *Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право*. 2013. № 3. С. 155–160.

7. Недохлєбов І. І. *Інформаційна безпека України в умовах сучасних загроз: організаційно-правові аспекти* : дис. … канд. юрид. наук : 12.00.07. Запоріжжя, 2024. 236 с.

8. Поліщук І. В. Особливості правового регулювання інформаційної безпеки в цивільній авіації України. *Юридичний вісник. Повітряне і космічне право*. 2020. № 2 (55). С. 27–32.

9. Садковський С. П. Деякі аспекти нормативно-правового забезпечення інформаційних технологій в контексті інформаційної безпеки України. *Юридичний науковий електронний журнал*. 2023. № 12. С. 121–123. DOI: https://doi.org/10.32782/2524-0374/2023-12/27.

10. Сидоркін П. Г., Горліченко С. О., Некоз В. С., Шилан М. В. Методи управління ризиками інформаційної безпеки CRAMM та COBIT 5 for Risk. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023. Т. 47, № 2. С. 41–47. DOI: https://doi.org/10.33099/2311-7249/2023-47-2-41-47.

11. Сугоняко Н. В. Інформаційна безпека в інформаційній діяльності суду. *Наукові записки Львівського університету бізнесу та права*. 2019. Т. 23. С. 195–200. DOI: https://doi.org/10.5281/zenodo.3678844.

12. Abdurrahman U. Correlation of Cyber Law with Civil Law: Theoretical and Practical Studies. *International Journal of Sustainability in Research*. 2023. Vol. 2, No. 1. P. 17–36. DOI: https://doi.org/10.59890/ijsr.v2i1.1146.

13. Contini F., Cordella A. Law and Technology in Civil Judicial Procedures // The Oxford Handbook of Law, Regulation and Technology / ed. by R. Brownsword, E. Scotford, K. Yeung. Oxford : Oxford University Press, 2017. Pp. 246–268. DOI: https://doi.org/10.1093/oxfordhb/9780199680832.013.47.

14. Del-Real C., Busser E., Berg B. A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies. *International Review of Law, Computers & Technology*. 2025. Vol. 3. DOI: https://doi.org/10.1080/13600869.2025.2457227.

15. Park S. Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics*. 2019. Vol. 58. Pp. 132–145. DOI: https://doi.org/10.1016/j.irle.2019.03.007.

16. Xu J. Research on the Civil Law Protection of Private Information. *Economics, Law and Policy*. 2025. Vol. 8, No. 2. Pp. 147–161. DOI: https://doi.org/10.22158/elp.v8n2p147.

17. Yeng P. K., Fauzi M. A., Sun L., Yang B. Assessing the Legal Aspects of Information Security Requirements for Health Care in 3 Countries: Scoping Review and Framework Development. *JMIR Human Factors*. 2022. Vol. 9, No. 2. DOI: https://doi.org/10.2196/30050.

Надійшла до редакції: 06.10.2025

Прийнята до опублікування: 13.12.2025

REFERENCES

1. Abdurrahman, U. (2023). Correlation of Cyber Law with Civil Law: Theoretical and Practical Studies. *International Journal of Sustainability in Research*, *2*(1), 17–36. https://doi.org/10.59890/ijsr.v2i1.1146.

2. Contini, F., & Cordella, A. (2017). Law and Technology in Civil Judicial Procedures. In R. Brownsword, E. Scotford, & K. Yeung (Eds.), *The Oxford Handbook of Law, Regulation and Technology* (pp. 246–268). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199680832.013.47.

3. Del-Real, C., Busser, E., & Berg, B. (2025). A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies. *International Review of Law, Computers & Technology*, *3*. https://doi.org/10.1080/13600869.2025.2457227.

4. Doronin, I. M. (2020). *Legal regulation of public relations in the sphere of national security in the information age* [Doctoral dissertation, Institute for Information Recording of the National Academy of Sciences of Ukraine].

5. Hurin, A. (2025, June 3). *Germany reports record level of cybercrime due to attacks by pro-Russian and anti-Israel hackers*. ZN,UA. https://zn.ua/ukr/europe/u-nimechchini-zajavili-pro-rekordnij-riven-kiberzlochinnosti-cherez-ataki-prorosijskikh-ta-antiizrajilskikh-khakeriv.html.

6. Kormych, B. A., Fedotov, O. P., & Averochkina, T. V. (2018). *Legal regulation of information activities*. National University “Odesa Law Academy”.

7. Nashynets-Naumova, A. Yu. (2013). Legal regulation of information security in civil aviation: international legal aspect. *Bulletin of the National Technical University of Ukraine "Kyiv Polytechnic Institute". Political Science. Sociology. Law*, *3*, 155–160.

8. Nashynets-Naumova, A. Yu. (2017). *Information security: issues of legal regulation*. Helvetyka.

9. Nedokhliebov, I. I. (2024). *Information security of Ukraine in the face of modern threats: organizational and legal aspects* [Candidate dissertation, Zaporizhzhia National University].

10. Park, S. (2019). Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics*, *58*, 132–145. https://doi.org/10.1016/j.irle.2019.03.007.

11. Polischuk, I. V. (2020). Features of legal adjusting of informative safety in civil aviation of Ukraine. *Scientific Works of National Aviation University. Series: Law Journal "Air and Space Law"*, *2*(55), 27–32.

12. Sadkovskyi, S. P. (2023). Some aspects of regulatory and legal support of information technologies in the context of information security of Ukraine. *Juridical Scientific and Electronic Journal*, *12*, 121–123. https://doi.org/10.32782/2524-0374/2023-12/27.

13. Suhoniatko, N. V. (2019). Information security in the court's information activities. *Scientific Notes of Lviv University of Business and Law*, *23*, 195–200. https://doi.org/10.5281/zenodo.3678844.

14. Sydorkin, P. H., Horlichenko, S. O., Nekoz, V. S., & Shylan, M. V. (2023). Methods of management of information security risks CRAMM and COBIT 5 for Risk. *Modern Information Technologies in the Sphere of Security and Defence*, *47*(2), 41–47. https://doi.org/10.33099/2311-7249/2023-47-2-41-47.

15. Xu, J. (2025). Research on the Civil Law Protection of Private Information. *Economics, Law and Policy*, *8*(2), 147–161. https://doi.org/10.22158/elp.v8n2p147.

16. Yeng, P. K., Fauzi, M. A., Sun, L., & Yang, B. (2022). Assessing the Legal Aspects of Information Security Requirements for Health Care in 3 Countries: Scoping Review and Framework Development. *JMIR Human Factors*, *9*(2). https://doi.org/10.2196/30050.

17. Zinchenko, O. I. (2024). European regional means of countering cyberterrorism. *Regional Studies*, *39*, 94–100. https://doi.org/10.32782/2663-6170/2024.39.15.

Received the editorial office: 6 October 2025

Accepted for publication: 13 December 2025

OLHA ANATOLYIVNA YAVOR,
Doctor of Law, Professor,
Yaroslav Mudryi National Law University (Kharkiv),
Department of Civil and Legal Policy,
Law of Intellectual Property and Innovations;
ORCID: https://orcid.org/0000-0002-5461-6498,
e-mail: yaroslava2527@gmail.com;

TATIANA SERHIIVNA KYRYCHENKO,
Candidate of Law, Associate Professor,
Kharkiv National University of Internal Affairs,
Educational and Scientific Institute No. 5,
Department of Civil Law and Procedure;
ORCID: https://orcid.org/0000-0002-8785-0475,
e-mail: ynatavesher021@gmail.com

CIVIL LAW MECHANISMS FOR REGULATING INFORMATION SECURITY AND RISK MANAGEMENT IN UKRAINE WITHIN THE CONTEXT OF EUROPEAN INTEGRATION

This article examines civil law mechanisms for regulating information security and risk management in Ukraine within the context of European integration. The information society and the mechanism of interaction between its components are identified and characterised. It is noted that the information society is the result of profound transformations in the fields of technology, economics and law, which are radically changing the nature of social and legal relations. The features of legal regulation of personal protection and risk management in the digital space in the context of European integration are analysed. The relevance and problems of modern mechanisms for ensuring information security, in particular in Ukraine, are examined, and the need to harmonise legislation with international standards, such as European Union

directives and Council of Europe conventions, is emphasised. Information security is interpreted as a system of legal and technical measures to protect the rights and interests of subjects in digital relations, with a particular emphasis on liability, compensation for damage and preventive measures. The role of civil law instruments in forming an effective protection system in the context of modern cyber threats and globalisation, which contributes to the improvement of the legal culture and legal stability of the Ukrainian information space, is examined.

It is noted that the modern understanding of information security in the context of civil law is formed at the intersection of national legislation, international standards and doctrinal approaches. Information security is considered not only as a sphere of public administration, but also as an important element of civil law relations that directly affects the rights of individuals and legal entities. Arguments are presented regarding the need to improve legal mechanisms, taking into account international standards and EU practice, particularly in the areas of risk management, contractual and insurance activities, which will contribute to increasing Ukraine's legal stability. It has been established that information security is becoming an important subject of civil law, and its protection requires the integration of technical, managerial and legal instruments.

It is proposed to supplement civil legislation and other regulatory acts regarding the civil law mechanism for regulating information security and risk management in Ukraine.

Keywords: *civil law regulation, mechanisms for protecting rights, information and legal relations, cyber threats, international cyber security standards, information security risks, legal liability, European integration.*

Цитування (ДСТУ 8302:2015): Явор О. А., Кириченко Т. С. Цивільно-правові механізми регулювання інформаційної безпеки та управління ризиками в Україні в контексті європейської інтеграції. *Право і безпека*. 2025. № 4 (99). С. 41–58. DOI: https://doi.org/10.32631/pb.2025.4.04.

Citation (APA): Yavor, O. A., & Kyrychenko, T. S. (2025). Civil Law Mechanisms for Regulating Information Security and Risk Management in Ukraine within the Context of European Integration. *Law and Safety, 4*(99), 41–58. https://doi.org/10.32631/pb.2025.4.04.