https://doi.org/10.26565/1684-8489-2025-2-21
УДК 351.9:004.056](477+4ЄС)

Боднар Катерина Віталіївна,
Doctor of Philosophy (PhD), Senior Lecturer at the Department of Public Policy, Postgraduate Student, Education and Research Institute of Public Administration, V. N. Karazin Kharkiv National University,
майдан Свободи, 4, м. Харків, 61022, Україна

e-mail: Ekaterina28051986@ukr.net *https://orcid.org/0000-0001-8512-1001*

РЕГУЛЯТОРНА АДАПТАЦІЯ СТАНДАРТІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ДО ГІБРИДНИХ ЗАГРОЗ В ЄС ТА УКРАЇНІ

Анотація. Досліджено напрями та механізми регуляторної адаптації стандартів захисту персональних даних до умов гібридних загроз у правових системах Європейського Союзу та України. Методологія дослідження базується на якісному аналізі первинних нормативних актів (GDPR, директиви NIS2 та CER, Регламент DORA, українське законодавство про захист персональних даних та кібербезпеку), офіційних документів інституцій ЄС, звітності ENISA та українських регуляторів із застосуванням порівняльно-правового методу та індуктивного узагальнення на основі конкретних інцидентів 2023–2024 років. Обґрунтовано, що традиційне розмежування між захистом персональних даних як елементом прав людини та кібербезпекою як технічною дисципліною втрачає актуальність: персональні дані перетворилися на інструмент «зброїзації ідентичності» для мікротаргетованих дезінформаційних кампаній, що підтверджується включенням ENISA маніпуляції інформацією до переліку основних загроз. Систематизовано регуляторну відповідь ЄС – багаторівневу архітектуру NIS2, DORA, CER та Cyber Resilience Act, яка інтегрує вимоги безпеки в операційну діяльність організацій та запроваджує персональну відповідальність керівництва за кіберризики. Виявлено чотири системні розриви в українському контексті: інституційний дисбаланс із домінуванням силового блоку над органами захисту даних; відсутність механізмів нагляду за обмеженнями прав у воєнний час; множинність режимів звітування без автоматичного обміну інформацією між відомствами; кадровий дефіцит фахівців з кібербезпеки. Доведено переважно реактивний характер регуляторної політики: атака на «Київстар» прискорила ухвалення Закону № 11290, атаки на державні реєстри – Постанову КМУ № 1531, тоді як євроінтеграційний законопроєкт № 8153 про захист персональних даних поступається пріоритетністю воєнному треку. Результати дослідження мають практичне значення для формування інтегрованої регуляторної політики, що поєднує захист прав суб'єктів даних із забезпеченням операційної стійкості державних інформаційних систем.

***Ключові слова**: захист персональних даних, гібридні загрози, кібербезпека, GDPR, NIS2, регуляторна адаптація.*

Як цитувати: Боднар К. В. Регуляторна адаптація стандартів захисту персональних даних до гібридних загроз в ЄС та Україні. *Актуальні проблеми державного управління*. 2025. № 2 (67). С. 419–436. https://doi.org/10.26565/1684-8489-2025-2-21

In cites: Bodnar, K.V. (2025). Regulatory Adaptation of Personal Data Protection Standards to Hybrid Threats in the EU and Ukraine. *Pressing Problems of Public Administration, 2 (67), 419–436.* https://doi.org/10.26565/1684-8489-2025-2-21 [in Ukrainian].

Постановка проблеми та актуальність теми дослідження. Цифрова трансформація публічного сектору впродовж останнього десятиліття радикально змінила архітектуру зберігання та обробки персональних даних громадян. Державні реєстри, що містять біометричні дані, відомості про власність, податкові записи та судові рішення, перетворилися на стратегічні об'єкти, вразливість яких безпосередньо загрожує функціонуванню держави. Водночас регуляторні режими захисту даних, сформовані переважно у відповідь на комерційні ризики та загрози приватності з боку технологічних корпорацій, виявилися недостатньо адаптованими до реалій гібридного протиборства. GDPR, ухвалений у 2016 році та імплементований з 2018 року, проєктувався для умов мирного часу і не враховував сценаріїв цілеспрямованих державно-спонсорованих атак на облікові системи критичної інфраструктури. Аналогічно, українське законодавство про захист персональних даних, яке перебуває у процесі гармонізації з європейськими стандартами через законопроєкт № 8153, змушене еволюціонувати в умовах безпрецедентного кібертиску [4].

Масштаб проблеми демонструють конкретні інциденти. У грудні 2024 року атака на державні реєстри Міністерства юстиції України, приписувана підрозділам ГРУ та хактивістському угрупованню XakNet, паралізувала роботу Єдиного державного реєстру юридичних осіб, реєстру актів цивільного стану та реєстру довіреностей. Наслідки охопили нотаріальну діяльність, операції з нерухомістю та реєстрацію шлюбів – функції, від яких залежить повсякденне життя мільйонів громадян. Цей епізод не є ізольованим: звіт ENISA Threat Landscape 2024 фіксує понад 11 тисяч кіберінцидентів за звітний період, з яких 322 одночасно зачепили дві або більше держав-членів ЄС. Публічна адміністрація залишається серед найбільш атакованих секторів (38% усіх інцидентів у 2024-2025 рр.), причому атаки на доступність систем та викрадення даних випереджають традиційні ransomware-загрози.

Регуляторна відповідь ЄС на ці виклики набуває системного характеру. Директива NIS2, ухвалена у листопаді 2022 року, розширила коло секторів, зобов'язаних імплементувати заходи кібербезпеки, до 180 тисяч організацій критичної інфраструктури. Директива CER (Critical Entities Resilience) від грудня того ж року запровадила вимоги щодо фізичної та операційної стійкості критичних суб'єктів. Стратегія ProtectEU, оприлюднена Європейською Комісією у квітні 2025 року, позиціонує захист персональних даних як невід'ємний елемент протидії гібридним загрозам. Водночас імплементація цих інструментів на національному рівні залишається нерівномірною, а координація між органами захисту даних та структурами кібербезпеки – фрагментарною.

Для України проблема набуває особливої гостроти через накладання євроінтеграційних зобов'язань, вимог воєнного стану та обмежених інституційних ресурсів. Уповноважений Верховної Ради з прав людини, який виконує функції органу захисту даних, видав рекомендації щодо балансування між національною безпекою та правами суб'єктів даних в умовах воєнного стану, проте системна нормативна база залишається у процесі формування. Законопроєкт № 8153, покликаний гармонізувати українське законодавство з GDPR та Конвенцією 108+, ухвалений у першо-

му читанні у листопаді 2024 року, однак його подальший розгляд конкурує з невідкладними воєнними пріоритетами парламентської порядки денної. Відтак виникає дослідницька проблема: яким чином регуляторні стандарти захисту персональних даних можуть бути адаптовані до умов гібридних загроз без компрометації фундаментальних прав громадян і водночас із забезпеченням операційної стійкості державних інформаційних систем?

Огляд літератури. Теоретичні засади європейського режиму захисту персональних даних сформовані працями провідних дослідників у сфері інформаційного права та регуляторного управління. Фундаментальний коментар до GDPR за редакцією К. Кунера, Л. Бігрейва та К. Доксі [26] залишається базовим джерелом для інтерпретації окремих статей Регламенту, особливо щодо територіального застосування, обов'язків контролерів та транскордонної передачі даних. О. Лінскі [27] у монографії обґрунтувала розмежування між правом на приватність та правом на захист даних як окремими, хоча й взаємопов'язаними, фундаментальними правами, що має безпосереднє значення для розуміння ризик-орієнтованого підходу GDPR. К. Юнг та Л. Бігрейв [38] у міждисциплінарному дослідженні проаналізували архітектуру регуляторного режиму через призму теорії управління, акцентуючи на дискреційних повноваженнях наглядових органів та проблемах їх легітимності. Б. Петкова [29] запропонувала концепцію захисту даних як «Першої поправки Європи», що підкреслює конституційний вимір цієї сфери. Серед досліджень впливу GDPR на практику обігу даних варто виділити роботи П. де Герта, Г. Мальг'єрі та співавторів [15] щодо права на портабельність даних, а також В. Восса та К. Гаузер [36] стосовно порівняння європейського та американського підходів до регулювання.

Проблематика гібридних загроз та їх впливу на інформаційну інфраструктуру розглядається у працях дослідників безпекових студій та критичної інфраструктури. Дж. Джаннопулос та колеги [23] у звіті Європейської комісії та Європейського оборонного агентства проаналізували ризики для енергетичного сектору в контексті гібридних операцій. М. Ротенберг [31] вивчив наслідки рішення Schrems II для трансатлантичної передачі даних в умовах загострення геополітичної конкуренції. Т. Райзінгер, І. Вагнер та Е. Бойтен [30] дослідили безпекові та приватнісні виклики уніфікованих комунікаційних систем. Звіти Агентства ЄС з кібербезпеки ENISA [19; 20] надають емпіричну базу для аналізу динаміки загроз: зокрема, фіксують зростання ролі state-nexus акторів, конвергенцію між хактивізмом та державно-спонсорованими операціями, а також використання DDoS-атак як інструменту впливу на електоральні процеси. С. Шастрі, М. Вассерман та В. Чідамбарам [33] проаналізували конфлікти між архітектурою хмарних систем та вимогами GDPR.

Серед українських дослідників проблематику кібербезпеки та захисту інформації в контексті національної безпеки активно розробляють науковці Інституту інформації, безпеки і права НАПрН України. О. Довгань [3] у серії аналітичних оглядів систематизує актуальні кіберзагрози для України в умовах збройної агресії, акцентуючи на вразливості державних інформаційних ресурсів. В. Фурашев [10] здійснив розмежування понять «кібербезпека» та «інформаційна безпека», що має методологічне значення для правового регулювання захисту даних у цифровому середовищі. Колектив авторів на

чолі з М. Ковалівим [8] дослідив правове забезпечення кібербезпеки критичної інформаційної інфраструктури України, включаючи державні реєстри та облікові системи. О. Гиляка [2] проаналізував співвідношення права на приватність та захисту персональних даних в умовах цифровізації, зокрема специфіку їх реалізації в українському правовому полі. Практичні аспекти кібербезпеки державних реєстрів висвітлені у публікаціях Державної служби спеціального зв'язку та захисту інформації України [7]. Водночас у літературі залишається недостатньо дослідженим питання адаптації регуляторних режимів захисту даних до умов активного збройного конфлікту та систематичних кібератак на облікові системи держави – лакуна, яку покликане заповнити це дослідження.

Мета і завдання статті. Мета дослідження – виявити напрями та механізми регуляторної адаптації стандартів захисту персональних даних до гібридних загроз у правових системах ЄС та України. Відповідно до мети, у статті вирішуються такі 2 завдання:

1) систематизувати нормативні та інституційні зміни у сфері захисту персональних даних ЄС та України, що є відповіддю на еволюцію гібридних загроз у період 2021–2025 років;

2) визначити розриви між регуляторними вимогами та реальною спроможністю наглядових органів забезпечувати захист персональних даних в умовах систематичних кібератак на державні облікові системи.

Методологія дослідження. Дослідження базується на якісній методології з використанням методів теоретичного синтезу та індуктивного узагальнення. Основу джерельної бази становлять первинні нормативні акти (GDPR, директиви NIS2 та CER, українське законодавство про захист персональних даних та кібербезпеку), офіційні документи інституцій ЄС (звіти ENISA, рішення Європейської ради, стратегія ProtectEU), а також звітність українських регуляторів (CERT-UA, Уповноважений з прав людини). Порівняльно-правовий аналіз застосовано для зіставлення регуляторних підходів ЄС та України, виявлення спільних тенденцій та специфічних відмінностей, зумовлених різним безпековим контекстом [4; 9].

Індуктивний метод використано для формулювання узагальнень на основі аналізу конкретних інцидентів (кібератаки на українські державні реєстри 2024 року, витоки даних у державах-членах ЄС) та регуляторних відповідей на них. Хронологічні рамки дослідження охоплюють період 2021–2025 років, що дозволяє простежити динаміку регуляторних змін від передвоєнного стану до актуального моменту. Географічні межі обмежені Європейським Союзом як джерелом базових стандартів та Україною як державою-кандидатом, що водночас є об'єктом інтенсивних гібридних операцій.

Виклад основного матеріалу. Співвідношення між захистом персональних даних та кібербезпекою упродовж останніх років зазнало помітних змін, і ці зміни потребують осмислення з позицій публічного управління. Історично ці дві сфери регулювалися окремо і виходили з різної логіки: захист персональних даних розглядався як елемент прав людини, спрямований на обмеження втручання держави та бізнесу в приватне життя особи, тоді як кібербезпека належала до технічної дисципліни захисту інформаційних систем від несанкціонованого доступу. GDPR 2016 р., який

став взірцем для багатьох національних законодавств, був орієнтований переважно на комерційний контекст: він регулював відносини між суб'єктами даних та компаніями, що ці дані обробляють, встановлюючи вимоги щодо згоди, мінімізації даних, права на забуття тощо. Питання державної безпеки та гібридних загроз у цьому регламенті присутні лише периферійно – у вигляді винятків для правоохоронних органів та служб безпеки [16].

Проте розвиток гібридних загроз упродовж 2021–2025 років поставив під сумнів доцільність такого розмежування. Європейський центр передового досвіду з протидії гібридним загрозам (Hybrid CoE) визначає ці загрози як скоординовані дії, що використовують вразливості демократичних інститутів через поєднання різних засобів – від кібератак до дезінформації [24]. Важливо, що в цьому визначенні акцентується саме на експлуатації вразливостей, а не на конкретних технічних методах атаки. Персональні дані громадян виявилися однією з таких вразливостей, причому їх роль змінилася якісно. Якщо раніше викрадення персональних даних мало переважно фінансову мотивацію – крадіжка коштів, шантаж, продаж баз даних на чорному ринку – то тепер агреговані дані використовуються для того, що дослідники називають «зброїзацією ідентичності» (weaponization of identities). Суть цього явища полягає в тому, що зібрані з різних джерел дані про релігійну, етнічну, політичну приналежність громадян дозволяють проводити мікротаргетовані дезінформаційні кампанії, спрямовані на поляризацію суспільства та підрив довіри до державних інституцій [9; 37].

Звіти ENISA за 2024 рік підтверджують цю тенденцію емпірично. Агентство включило «маніпуляцію інформацією та втручання» (FIMI) до переліку семи основних загроз, поставивши її поряд з атаками на доступність систем та програмами-вимагачами [19]. Це рішення відображає не просто розширення переліку загроз, а визнання того, що цілісність даних – їх захист від несанкціонованої модифікації та маніпуляції – стає не менш важливою, ніж конфіденційність. Особливу небезпеку, за оцінкою ENISA, становить поєднання викрадених персональних даних з технологіями генеративного штучного інтелекту, що дозволяє створювати переконливі дипфейки та проводити автоматизовані кампанії соціальної інженерії у масштабах, недосяжних для людини-оператора [19; 20]. Ці висновки мають практичне значення для регуляторної політики: вони означають, що захист персональних даних не може обмежуватися лише забезпеченням конфіденційності та отриманням згоди на обробку, а має включати заходи із захисту інфраструктури, яка ці дані зберігає та обробляє.

Відповіддю Європейського Союзу на ці виклики стало ухвалення низки нормативних актів, які інтегрують вимоги безпеки в операційну діяльність організацій. Директива NIS2, що замінила попередню директиву NIS1, набула чинності 16 січня 2023 року і встановила дедлайн для транспозиції у національне законодавство держав-членів до 17 жовтня 2024 року [16]. Порівняння цих двох директив показує напрям руху регуляторної думки. NIS1 2016 року охоплювала обмежене коло секторів і залишала державам-членам значну свободу розсуду при визначенні операторів основних послуг. NIS2 радикально розширила коло регульованих суб'єктів до 18 секторів, включивши не лише традиційні енергетику, транспорт, охорону здоров'я та банківську справу, але й управління відходами, виробництво хімічних

речовин та продуктів харчування, поштові та кур'єрські послуги, державне управління, космос [16]. Практичне значення цього розширення полягає в тому, що величезні масиви персональних даних, які раніше підпадали лише під режим GDPR, тепер регулюються паралельно двома режимами: GDPR встановлює вимоги щодо прав суб'єктів даних, а NIS2 – щодо захисту інфраструктури, яка ці дані обробляє.

Увагу заслуговує стаття 23 Директиви NIS2, яка встановила каскадну систему звітування про інциденти. Ця система передбачає три етапи: раннє попередження національної команди реагування (CSIRT) протягом 24 годин після виявлення інциденту, оновлена інформація з оцінкою серйозності протягом 72 годин, повний звіт з аналізом причин та вжитих заходів протягом місяця [28]. Важливо зіставити ці вимоги з аналогічними нормами GDPR: стаття 33 останнього також вимагає повідомлення наглядового органу про витік персональних даних протягом 72 годин. На практиці більшість кіберінцидентів зачіпають обидва аспекти одночасно: атака на інформаційну систему зазвичай означає і загрозу для персональних даних, що в ній зберігаються. Це створює для організацій необхідність синхронізувати процеси звітування різним регуляторам і уникати суперечливих свідчень, що є нетривіальним управлінським завданням в умовах кризи [16].

Ще однією важливою новацією NIS2 стало запровадження персональної відповідальності вищого керівництва організацій за невиконання зобов'язань з управління кіберризиками. Директива передбачає, що санкції можуть включати не лише адміністративні штрафи для юридичних осіб, але й тимчасову заборону для фізичних осіб займати керівні посади [35]. Ця норма є новою для права ЄС у сфері кібербезпеки і змінює ставлення корпоративного управління до питань інформаційної безпеки: з технічної функції, делегованої IT-департаменту, кібербезпека перетворюється на стратегічний ризик, який має контролюватися радою директорів.

Паралельно з NIS2 було ухвалено Регламент DORA (Digital Operational Resilience Act), який став повністю застосовним з 17 січня 2025 року [22]. DORA є спеціальним режимом для фінансового сектору і відрізняється від NIS2 за юридичною формою: це регламент прямої дії, а не директива, що виключає варіативність при імплементації у національне законодавство. Зміст DORA зосереджений на управлінні ризиками, пов'язаними з постачальниками послуг ІКТ, що відображає реальність сучасної фінансової індустрії, де банки масово мігрують у хмарні середовища і стають залежними від обмеженого кола провайдерів. Регламент встановлює вимоги до контрактів з хмарними провайдерами та, що важливо, надає європейським наглядовим органам повноваження безпосередньо перевіряти цих провайдерів [22]. DORA також запроваджує обов'язкове тестування на проникнення, що базується на загрозах (TLPT), яке передбачає симуляцію реальних атак на виробничі системи. Це створює напругу із захистом персональних даних, оскільки тестувальники – часто зовнішні підрядники – отримують доступ до реальних банківських даних клієнтів, і регламент вимагає спеціальних заходів для мінімізації цих ризиків.

Для України ця європейська регуляторна архітектура створює ситуацію, яку варто чесно визнати. З одного боку, Угода про асоціацію та курс на членство в ЄС формально зобов'язують нас імплементувати весь цей масив

норм – NIS2, елементи DORA для фінансового сектору, стандарти ENISA. З іншого боку, ми спостерігаємо, як адміністрація Трампа системно тисне на європейських союзників, ставлячи під сумнів трансатлантичну солідарність і просуваючи дерегуляційну логіку, діаметрально протилежну європейському підходу. Це створює для України не просто технічну проблему імплементації, а стратегічну дилему позиціонування. Якщо ми сприймаємо європейські стандарти як формальну вимогу для «галочки» – ми втрачаємо час і ресурси на бюрократію без реального захисту. Якщо ж ми використовуємо цей момент для побудови власної інституційної спроможності у сфері кібербезпеки – ми отримуємо конкурентну перевагу незалежно від того, як еволюціонуватимуть трансатлантичні відносини. Практично це означає, що українські органи публічної влади та критична інфраструктура вже зараз мають готуватися до каскадних систем звітування, персональної відповідальності керівників за кіберінциденти, регулярного тестування на проникнення – не тому, що цього вимагає Брюссель, а тому, що війна зробила ці практики питанням виживання. Іронія полягає в тому, що українські енергетичні компанії, банки, державні реєстри вже де-факто живуть в режимі, жорсткішому за NIS2, – постійних атак, обмежених ресурсів, необхідності миттєвого реагування. Вважаю, що на наступні 4-5 років для України критичними стають такі напрями:

1) створення національної CSIRT-інфраструктури, здатної забезпечити 24/72-годинні цикли звітування без паралічу операційної діяльності;

2) розробка механізмів одночасного виконання вимог захисту персональних даних (українського аналога GDPR) та кібербезпекових стандартів без дублювання бюрократії;

3) формування кадрового резерву керівників, які розуміють кібербезпеку як стратегічний, а не технічний ризик;

4) побудова системи контролю за хмарними провайдерами, особливо з огляду на залежність від американських платформ в умовах непередбачуваності політики США.

Архітектуру регуляторних змін ЄС доповнюють Директива CER (Critical Entities Resilience), яка закриває прогалину у фізичному захисті інфраструктури, та Cyber Resilience Act, що набув чинності в грудні 2024 року [34, 21]. CER враховує загрози, які виходять за межі кіберпростору: природні катастрофи, тероризм, саботаж. Cyber Resilience Act встановлює обов'язкові вимоги кібербезпеки для продуктів з цифровими елементами протягом їх життєвого циклу, закріплюючи принцип «security by design», який є дзеркальним відображенням принципу «privacy by design» із GDPR. Разом ці акти формують багаторівневу систему, де захист даних, захист інфраструктури та безпека продуктів взаємно підсилюють один одного.

Український контекст суттєво відрізняється від європейського, хоча й перебуває під його впливом. Україна опинилася в ситуації, коли необхідність гармонізації законодавства з ЄС як країни-кандидата накладається на реалії війни. Це призвело до формування двох паралельних регуляторних треків, які розвиваються з різною швидкістю та різною логікою. Перший трек – євроінтеграційний – представлений законопроектом № 8153 «Про захист персональних даних», поданим до Верховної Ради у жовтні 2022 року. Цей законопроект покликаний замінити застарілий Закон 2010 року, який базу-

вався на Директиві 95/46/ЄС – попередниці GDPR, що втратила чинність ще у 2018 році. Розгляд законопроекту затягнувся через пріоритетність оборонного законодавства: лише 20 листопада 2024 року парламент ухвалив його у першому читанні [25].

Законопроект № 8153 імплементує архітектуру GDPR майже повністю: вводить термінологію «контролер» та «оператор» замість застарілих «володілець» та «розпорядник», закріплює право на забуття та право на мобільність даних, встановлює обов'язок призначати відповідального за захист даних (DPO) для певних категорій суб'єктів, передбачає процедуру оцінки впливу на захист даних (DPIA) для високоризикових обробок [5]. Законопроект також чітко визначає, що мовчання, попередньо проставлені галочки або бездіяльність не можуть вважатися згодою на обробку персональних даних [1]. Ця норма, яка відтворює відповідне положення GDPR, потребуватиме перегляду маркетингових практик та інтерфейсів користувача для значної частини українського бізнесу. Проте темпи розгляду законопроекту свідчать про те, що євроінтеграційний трек поступається пріоритетністю перед воєнним.

Другий трек – воєнний – представлений Законом № 11290, ухваленим Верховною Радою у березні 2025 року та підписаним Президентом у квітні того ж року [6]. Цей закон є прямою відповіддю на конкретні інциденти, насамперед на атаку на державні реєстри Міністерства юстиції наприкінці 2024 року. Закон структурує Національну систему реагування на кіберінциденти, визначаючи ієрархію органів: CERT-UA стає центральним координуючим органом на національному рівні, створюються галузеві центри кіберзахисту, формуються служби кіберзахисту на підприємствах критичної інфраструктури [14]. Дискусійною нормою стало положення про обов'язкове погодження кандидатур офіцерів з кібербезпеки (CISO) в органах влади та на об'єктах інфраструктури з Державною службою спеціального зв'язку та захисту інформації [6]. Представники громадянського суспільства критикували цю норму, вказуючи на ризик надмірного впливу спецслужб та можливе гальмування цифровізації через бюрократичні процедури [12]. Закон також надає державі повноваження втручатися в управління мережами приватних операторів у разі інцидентів, що загрожують національній безпеці, фактично імплементуючи концепцію активної кібероборони на законодавчому рівні [14].

Доповненням до Закону № 11290 стала Постанова КМУ № 1531 від 26 листопада 2025 року, яка затвердила єдиний стандарт кіберзахисту для державних органів. Ця постанова фіксує відхід від системи КСЗІ (Комплексна система захисту інформації), яка існувала з радянських часів і критикувалася за формалізм: на практиці вона зводилася переважно до «паперової безпеки» – оформлення документів та проходження атестацій без реального підвищення рівня захисту. Новий стандарт базується на ризик-орієнтованому підході, вимагаючи від керівників планувати витрати на кіберзахист виходячи з реальних загроз конкретної організації.

Аналіз конкретних інцидентів дозволяє зрозуміти логіку регуляторних рішень та виявити вразливості, які вони покликані усунути. Атака на оператора мобільного зв'язку «Київстар» 12 грудня 2023 року стала переломним моментом у сприйнятті кіберзагроз в Україні. Атака призвела

до повного відключення послуг для 24 мільйонів абонентів, паралізувавши не лише мобільний зв'язок, але й пов'язані з ним сервіси: не працювали термінали оплати, системи оповіщення про повітряну тривогу в деяких регіонах, банківські SMS-повідомлення. Відповідальність за атаку взяло угруповання «Солнцепек», яке спецслужби України та західних країн ідентифікують як структуру російського ГРУ, пов'язану з групою Sandworm/APT44 [32].

Розслідування атаки виявило кілька важливих обставин. По-перше, зловмисники перебували в мережі оператора щонайменше з травня 2023 року – понад півроку до активної фази атаки. Первинний доступ було отримано через скомпрометований обліковий запис одного зі співробітників, що підтвердив генеральний директор компанії [13]. Ця обставина вказує на обмеження периметрального захисту: навіть найсучасніші міжмережеві екрани не захищають від загрози, яка вже перебуває всередині мережі. По-друге, хоча компанія офіційно заперечила витік персональних даних клієнтів, представники СБУ зазначили, що хакери з таким рівнем доступу могли перехоплювати SMS, визначати геолокацію абонентів та викрадати акаунти месенджерів [32]. Це означає, що навіть за відсутності публічного витоку даних – публікації баз у даркнеті – інформація могла бути використана ворожою розвідкою для цільового спостереження та, потенційно, для коригування вогню. Інцидент продемонстрував, що критична інфраструктура приватного сектору може бути «єдиною точкою відмови», здатною паралізувати життя країни, і став каталізатором для прискорення ухвалення Закону № 11290.

Атаки на державні реєстри Міністерства юстиції наприкінці 2024 року мали інший характер, але не менш серйозні наслідки. Внаслідок атаки було призупинено роботу близько 25 реєстрів, включаючи реєстри нерухомості, бізнесу та актів цивільного стану [17]. Практичні наслідки полягали в тому, що нотаріат фактично зупинився: громадяни не могли оформити купівлю-продаж нерухомості, вступити у спадщину, змінити власника компанії. Ці реєстри є серцем цифрової держави – без них неможливе функціонування цивільного обороту. Криза виявила проблеми в управлінні державним підприємством «Національні інформаційні системи» (НАІС), яке адмініструє реєстри: Міністерство юстиції було змушене звільнити керівництво підприємства та провести аудит безпеки [12]. Цей випадок став аргументом на користь централізації контролю за кадровими призначеннями в сфері кібербезпеки, що згодом було закріплено в Законі № 11290.

Динаміка кіберінцидентів в Україні відображає загальну тенденцію до інтенсифікації: якщо у 2021 році CERT-UA зафіксувала близько 1350 інцидентів, то у 2024 році їх кількість досягла 4315, що становить зростання на 70% порівняно з 2023 роком [14]. Змінився і характер атак: від wiper-атак 2022 року, спрямованих на знищення даних і порушення роботи систем, до складніших операцій 2024 року, орієнтованих на використання даних для соціальної інженерії та розвідувальних цілей. Ця еволюція підтверджує тезу про «зброїзацію ідентичності»: дані стають цінними не стільки самі по собі, скільки як інструмент впливу.

Аналіз виявляє кілька системних розривів між регуляторними вимогами та реальними можливостями їх виконання. Перший розрив – інституційний

дисбаланс між органами кібербезпеки та органами захисту даних. В Україні Офіс Уповноваженого Верховної Ради з прав людини формально є регулятором у сфері захисту персональних даних, проте його спроможність обмежена. Кількість звернень до Офісу у 2024 році зросла на 29% і досягла 123 221, значна частина яких стосується порушень прав військовослужбовців та захисту даних [11]. При цьому Офіс не має права самостійно накладати адміністративні штрафи – це робить суд – і не володіє технічним ресурсом для розслідування складних кіберінцидентів. З ухваленням Закону № 11290 Держспецзв'язку та СБУ отримали розширені повноваження щодо контролю за інформаційними системами, і центр прийняття рішень щодо безпеки даних фактично змістився до силового блоку. Цей дисбаланс створює ризик того, що питання захисту даних розглядатимуться виключно через призму державної безпеки, тоді як права індивіда відходитимуть на другий план. Відсутність незалежного органу захисту даних з повноваженнями, аналогічними європейським, залишається одним із зауважень Європейської Комісії до України в контексті євроінтеграції.

Другий розрив пов'язаний з обмеженням прав у воєнний час. Упродовж 2022–2025 років Україна регулярно подавала нотифікації до Ради Європи відповідно до статті 15 Європейської конвенції про захист прав людини, повідомляючи про обмеження прав, передбачених статтею 8 (право на повагу до приватного життя), у зв'язку з воєнним станом. Це створює зону, де спецслужби можуть здійснювати перехоплення комунікацій та збір даних без судових санкцій, які були б необхідні в мирний час. Хоча таке обмеження виправдане обставинами війни, відсутність чітких механізмів нагляду та положень про автоматичне припинення дії (sunset clauses) створює ризик закріплення надзвичайних повноважень на невизначений термін після завершення активної фази конфлікту.

Третій розрив – множинність режимів звітування. Організації в Україні зобов'язані звітувати до CERT-UA про кіберінциденти відповідно до Закону № 11290, до НБУ (для банків) відповідно до постанов регулятора, а в перспективі – до регулятора захисту даних про витоки персональних даних після ухвалення Закону № 8153. Директива NIS2 передбачає створення «єдиного вікна» для уникнення дублювання звітів, однак в Україні механізм автоматичного обміну інформацією між відомствами існує лише номінально, що створює надмірне адміністративне навантаження на організації під час кризових ситуацій.

Четвертий розрив – кадровий дефіцит. Вимога Закону № 11290 про наявність фахівців з кібербезпеки в органах влади та на об'єктах інфраструктури стикається з реальністю ринку праці. За даними ENISA, глобальний дефіцит фахівців з кібербезпеки становить 3–4 мільйони осіб [19]. В Україні ситуація ускладнюється тим, що державний сектор не може конкурувати зарплатами з приватним, а приватний – з міжнародним аутсорсингом. За таких умов вимога про призначення кваліфікованих CISO ризикує перетворитися на формальність, коли відповідальність покладатиметься на системних адміністраторів без належних компетенцій (рис. 1).

Порівняння регуляторних підходів ЄС та України виявляє як спільні тенденції, так і відмінності, зумовлені різним безпековим контекстом. За критеріями визначення суб'єктів регулювання обидві системи

демонструють схожість: ЄС застосовує поділ на «важливі» та «значущі» суб'єкти з охопленням 18 секторів, Україна використовує систему критичної інфраструктури з чотирма категоріями критичності. Щодо звітування підходи дещо різняться: ЄС акцентує на структурованому процесі (24 год – 72 год – 1 міс), тоді як Україна робить акцент на оперативності з вимогою негайного повідомлення. В питаннях відповідальності керівників обидві системи рухаються в одному напрямі: ЄС передбачає штрафи та заборону на посади, Україна – адміністративну та кримінальну відповідальність посадових осіб.

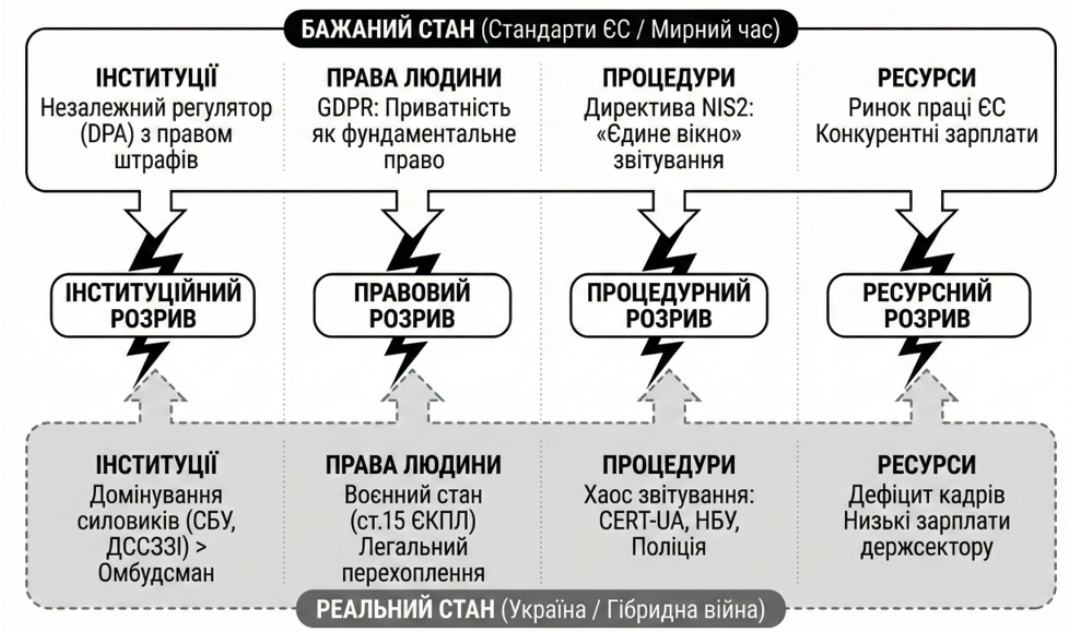

Рисунок 1. Системні розриви (regulatory gaps) адаптації стандартів захисту даних в Україні до гібридних загроз у 2022-2026 рр.

Figure 1. Regulatory gaps in the adaptation of data protection standards in Ukraine to hybrid threats in 2022-2026.

**Джерело: складено авторкою.*

**Source: compiled by the author.*

Найбільш помітна відмінність спостерігається в інституційному нагляді. Європейська модель базується на мережі національних команд реагування з координацією ENISA та на співпраці з незалежними органами захисту даних. Українська модель характеризується централізацією та домінуванням силового блоку – CERT-UA, Держспецзв'язку, СБУ. Щодо контролю ланцюгів постачання Україна застосовує заборони за критерієм країни походження (заборона російського програмного забезпечення), тоді як ЄС використовує ризик-орієнтований підхід без прямих географічних заборон (табл. 1).

Таблиця. – Механізми «Брюссельського ефекту» GDPR та їх диференційована дія на пострадянські країни

Table. – Mechanisms of the "Brussels Effect" of the GDPR and their differentiated impact on post-Soviet countries

Вимір впливу **Measuring impact**	**Як працює механізм** **How the mechanism works**	**Що визначає результативність** **What determines effectiveness**
Ринкова гравітація **Market gravity**	Компанії, що прагнуть на ринок ЄС (450 млн споживачів, $15 трлн ВВП), змушені добровільно прийняти стандарти GDPR навіть без формальних зобов'язань – економічна доцільність переважає над юрисдикційними бар'єрами	Інтенсивність цифрової торгівлі з ЄС: що більший обсяг IT-експорту, то сильніший тиск на гармонізацію (Грузія, Молдова демонструють вищу чутливість через IT-сектор як драйвер економіки)
Технологічна неподільність **Technological indivisibility**	Цифрові продукти є глобальними за природою – створювати окремі версії з різними політиками приватності для різних ринків технологічно та економічно недоцільно, тому застосовується найвищий стандарт для всіх	Залежність від іноземних технологічних рішень та платформ: локальні оператори, інтегровані у глобальні екосистеми, автоматично імпортують GDPR-стандарти через supply chain
Примусовий потенціал **Coercive potential**	Штрафи до 4% глобального річного обороту створюють «довге плече» європейського права – навіть компанії без фізичної присутності в ЄС підпадають під санкції за порушення прав європейців	Правозастосовна спроможність національних регуляторів: слабкі омбудсмени (Україна) чи нестабільні органи (Молдова) не здатні забезпечити реальний enforcement навіть прогресивних законів
Інституційна рецепція **Institutional reception**	Формальне копіювання норм GDPR у національне законодавство може залишатись «паперовим тигром» без перебудови бюрократичних рутин, бізнес-моделей та суспільних настанов	Культурна дистанція від європейських цінностей індивідуалізму: пострадянська парадигма захисту даних як функції держави (а не права людини) гальмує змістовну трансформацію
Соціальне укорінення	Стійкість регуляторних змін залежить від того, чи сприймає суспільство приватність як фундаментальну цінність – без цього бізнес бачить GDPR як «регуляторний тягар», а не конкурентну перевагу	Рівень правової грамотності та проактивність громадян як суб'єктів захисту даних: там, де населення байдуже до privacy (Україна), регулятори позбавлені суспільної підтримки

**Джерело: розробка авторки.*
**Source: author's own work.*

На підставі проведеного аналізу можна сформулювати кілька узагальнень.

– По-перше, традиційне розмежування між захистом персональних даних та кібербезпекою втрачає актуальність під тиском гібридних загроз. Дані стають не лише об'єктом захисту прав людини, але й елементом національної безпеки, що вимагає інтегрованих регуляторних підходів.

– По-друге, обидві досліджувані системи – і європейська, і українська – демонструють розрив між законодавчими цілями та реальними

можливостями наглядових органів. В Україні цей розрив поглиблюється воєнними обставинами та ресурсними обмеженнями.

– По-третє, більшість нормативних змін має реактивний характер: атака на «Київстар» прискорила ухвалення Закону № 11290, атаки на реєстри – Постанову № 1531.

Це свідчить про те, що регуляторна політика в цій сфері переважно відповідає на вже виявлені загрози, а не випереджає їх.

Висновки з даного дослідження і перспективи подальших досліджень.

На основі проведених вище аналізу, синтезу і власних роздумів, можна зробити такі висновки.

1) Традиційне розмежування між захистом персональних даних як елементом прав людини та кібербезпекою як технічною дисципліною втрачає актуальність під тиском гібридних загроз. Емпіричні дані ENISA про включення «маніпуляції інформацією та втручання» (FIMI) до переліку семи основних загроз підтверджують: персональні дані перетворилися на інструмент «зброїзації ідентичності», коли агреговані відомості про релігійну, етнічну, політичну приналежність громадян використовуються для мікротаргетованих дезінформаційних кампаній. Це означає, що регуляторна політика захисту даних має інтегрувати вимоги щодо захисту інфраструктури, а не обмежуватися забезпеченням конфіденційності та отриманням згоди на обробку.

2) Аналіз виявляє чотири системні розриви між регуляторними вимогами та реальною спроможністю їх виконання в Україні: інституційний дисбаланс між органами кібербезпеки та захисту даних із фактичним зміщенням центру прийняття рішень до силового блоку; відсутність чітких механізмів нагляду за обмеженнями прав у воєнний час та положень про автоматичне припинення надзвичайних повноважень; множинність режимів звітування без механізму автоматичного обміну інформацією між відомствами; кадровий дефіцит, що перетворює вимогу про призначення кваліфікованих CISO на формальність. Ці розриви поглиблюються воєнними обставинами та ресурсними обмеженнями.

3) Порівняльний аналіз регуляторних підходів ЄС та України демонструє принципову відмінність в інституційних моделях нагляду. Європейська модель базується на мережі національних команд реагування з координацією ENISA та на співпраці з незалежними органами захисту даних. Українська модель характеризується централізацією та домінуванням силового блоку – CERT-UA, Держспецзв'язку, СБУ. Водночас Україна де-факто функціонує в режимі, жорсткішому за NIS2: постійні атаки, обмежені ресурси, необхідність миттєвого реагування. Це створює майже «парадокс», коли практика випереджає нормативну базу, але без належного інституційного закріплення.

4) Підтверджується переважно реактивний характер регуляторної політики у сфері захисту даних: атака на «Київстар» у грудні 2023 року прискорила ухвалення Закону № 11290, атаки на державні реєстри Міністерства юстиції наприкінці 2024 року – Постанову КМУ № 1531. Законопроєкт № 8153 про захист персональних даних, покликаний гармонізувати законодавство з GDPR, ухвалений у першому читанні лише через два роки після подання, оскільки євроінтеграційний трек поступається пріоритетніс-

тю воєнному. Це свідчить про те, що регуляторна політика відповідає на вже виявлені загрози, а не випереджає їх.

5) Перспе*ктиви подальших досліджень* пов'язані з необхідністю емпіричної оцінки ефективності централізованої моделі кіберзахисту після повноцінної імплементації Закону № 11290 та аналізом механізмів відновлення балансу між безпековими повноваженнями держави та правами суб'єктів даних після завершення воєнного стану. Окремого вивчення потребує питання розробки «sunset clauses» – нормативних положень про автоматичне припинення надзвичайних повноважень, які б запобігали закріпленню воєнних обмежень приватності на невизначений термін у післявоєнному правовому порядку України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гаврилюк А. GDPR по-українськи: ключові аспекти ЗП № 8153 «Про захист персональних даних». Sayenko Kharenko. 2024. URL: https://sk.ua/uk/gdpr-po-ukrainski-kljuchovi-aspekti-zp-8153-pro-zahist-personalnih-danih/ (дата звернення: 18.06.2025).
2. Гиляка О. С. Право на приватність та захист персональних даних в умовах цифровізації. *Вісник Національної академії правових наук України.* 2023. Т. 30. № 1. С. 15–32. https://doi.org/10.31359/1993-0909-2023-30-1-15
3. Довгань О. Д. (упоряд.). Кібербезпека в інформаційному суспільстві: інформаційно-аналітичний дайджест. Київ: Інститут інформації, безпеки і права НАПрН України; Національна бібліотека України ім. В. І. Вернадського, 2023. № 10. 320 с.
4. Дунаєв І., Луговенко Н. Держава і персональні дані у світі post-GDPR: на шляху до глобального консенсусу чи фрагментації регулювання? *Теорія та практика державного управління*. 2024. Т. 2. № 79. С. 28–62. https://doi.org/10.26565/1727-6667-2024-2-02
5. ЄБА. Обговорення законопроєкту № 8153 «Про захист персональних даних». Київ, 2025. URL: https://eba.com.ua/obgovorennya-zakonoproyektu-8153-pro-zahyst-personalnyh-danyh/ (дата звернення: 18.06.2025).
6. Жахалов Я. В Україні реформують кіберзахист після атаки на реєстри. Це розширить повноваження Держспецзв'язку. DOU. 2025. URL: https://dou.ua/lenta/news/new-law-on-cybersecurity/ (дата звернення: 18.06.2025).
7. Звіт про стан кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури у 2023 році. Київ : Державна служба спеціального зв'язку та захисту інформації України, 2024. 45 с.
8. Ковалів М., Скриньковський Р., Назар Ю., Єсімов С., Красницький І., Кайдрович Х., Князь С., Кемська Ю. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. *Path of Science*. 2021. Vol. 7. No. 4. P. 2011–2018. https://doi.org/10.22178/pos.69-12
9. Удовенко О. В., Величко Л. Ю. Як формує «Брюсельський ефект» нові стандарти? Вплив стандарту захисту персональних даних GDPR та інших ініціатив ЄС на Україну та країни поза Євросоюзом. *Актуальні проблеми державного управління*. 2024. Т. 2. № 65. С. 187–215. https://doi.org/10.26565/1684-8489-2024-2-10
10. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. № 2. С. 162–169.
11. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні за 2024 рік. Київ: Офіс Омбудсмана, 2025. 312 с. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/1-eng-web.pdf (дата звернення: 18.06.2025).
12. Ярмоленко О., Гусєв Г. Держава реформує кіберзахист після масштабного зламу. Держспецзв'язку отримає нові повноваження – і цю службу знову критикують. «Бабель» пояснює суть реформи і просить її автора відповісти на критику. Київ, 2025. URL: https://babel.ua/texts/116673-derzhava-reformuye-kiberzahist-pislya-masshtabnogo-zlamu-derzhspeczv-yazku-otrimaye-novi-povnovazhennya-i-cyu-sluzhbu-znovu-kritikuyut-babel-poyasnyuye-sut-reformi-i-prosit-jiji-avtora-vidpovisti-na-k (дата звернення: 18.06.2025).

13. Bepon K. 5 Questions (and Answers) About the Kyivstar Attack. KELA Cyber. 2024. URL: https://www.kelacyber.com/blog/5-questions-and-answers-about-the-kyivstar-attack/ (дата звернення: 18.06.2025).

14. CERT-UA recorded 4,315 cyber incidents in 2024. Державна служба спеціального зв'язку та захисту інформації України. 2025. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 18.06.2025).

15. De Hert P., Papakonstantinou V., Malgieri G., Beslay L., Sanchez I. The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services. *Computer Law & Security Review.* 2018. Vol. 34. No. 2. P. 193–203. https://doi.org/10.1016/j.clsr.2017.10.003

16. 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. *Official Journal of the European Union*. L 333. 2022. P. 80–152.

17. Due to Russia's cyberattack, all registration actions are unavailable, about 25 state registers suspended. Interfax-Ukraine. 2024. URL: https://en.interfax.com.ua/news/general/1036066.html (дата звернення: 18.06.2025).

18. ENISA. Report on the State of Cybersecurity in the Union 2024. Athens: ENISA, 2024. 71 p. https://doi.org/10.2824/0401593

19. ENISA Threat Landscape 2024. Athens: European Union Agency for Cybersecurity, 2024. 131 p. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 18.06.2025).

20. ENISA Threat Landscape 2025. Athens: European Union Agency for Cybersecurity, 2025. 148 p. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (дата звернення: 18.06.2025).

21. EU Cyber Resilience Act takes effect, brings new era of mandatory cybersecurity standards for digital products. Industrial Cyber. 2024. URL: https://industrialcyber.co/regulation-standards-and-compliance/eu-cyber-resilience-act-takes-effect-brings-new-era-of-mandatory-cybersecurity-standards-for-digital-products/ (дата звернення: 18.06.2025).

22. European Union Data Privacy: What's Next for 2025? TrustArc. 2025. URL: https://trustarc.com/resource/european-union-data-privacy-whats-next-for-2025/ (дата звернення: 18.06.2025).

23. Giannopoulos G., Smith H., Theocharidou M. The Landscape of Hybrid Threats: A Conceptual Model. Luxembourg: Publications Office of the European Union, 2023. 48 p.

24. Hybrid threats as a concept. Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats. URL: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (дата звернення: 18.06.2025).

25. Investment Climate Statements 2025: Ukraine. U.S. Department of State. 2025. URL: https://www.state.gov/reports/2025-investment-climate-statements/ukraine (дата звернення: 18.06.2025).

26. Kuner C., Bygrave L. A., Docksey C. (eds.). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020. 1393 p.

27. Lynskey O. The Foundations of EU Data Protection Law. Oxford: Oxford University Press, 2015. 289 p.

28. NIS 2 Directive, Article 23: Reporting obligations. URL: https://www.nis-2-directive.com/NIS_2_Directive_Article_23.html (дата звернення: 18.06.2025).

29. Petkova B. Privacy as Europe's First Amendment. *European Law Journal*. 2019. Vol. 25. No. 2. P. 140–154. https://doi.org/10.1111/eulj.12316

30. Reisinger T., Wagner I., Boiten E. A. Security and Privacy in Unified Communication. *ACM Computing Surveys.* 2022. Vol. 55. No. 3. P. 1–35. https://doi.org/10.1145/3498335

31. Rotenberg M. Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection. *European Law Journal.* 2020. Vol. 26, No. 1–2. P. 141–152. https://doi.org/10.1111/eulj.12370

32. Russian Sandworm hackers breach Kyivstar network, causing devastating damage and signaling warning to the West. Industrial Cyber. 2024. URL: https://industrialcyber.co/threat-landscape/russian-sandworm-hackers-breach-kyivstar-network-causing-devastating-damage-and-signaling-warning-to-the-west/ (дата звернення: 18.06.2025).

33. Shastri S., Wasserman M., Chidambaram V. How Design and Operation of Modern Cloud-Scale Systems Conflict with GDPR. *Proceedings of the 2021 ACM Symposium on Cloud Computing.* 2021. P. 560–566.

34. The EU Critical Entities Resilience Directive – What is the impact on your organisation? Osborne Clarke. 2024. URL: https://www.osborneclarke.com/insights/eu-critical-entities-resilience-directive-what-impact-your-organisation (дата звернення: 18.06.2025).

35. The NIS 2 Directive: Updates, Compliance, Training. URL: https://www.nis-2-directive.com/ (дата звернення: 18.06.2025).

36. Voss W. G., Houser K. Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal.* 2019. Vol. 56, No. 2. P. 287–344. https://doi.org/10.1111/ablj.12139

37. Weaponizing social Identities: What can we learn from examples of targeted disinformation? Hybrid CoE. 2024. URL: https://www.hybridcoe.fi/news/weaponizing-social-identities-what-can-we-learn-from-examples-of-targeted-disinformation/ (дата звернення: 18.06.2025).

38. Yeung K., Bygrave L. A. Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance.* 2022. Vol. 16. No. 1. P. 137–168. https://doi.org/10.1111/rego.12401

Стаття надійшла до редакції 27.07.2025 р.
Стаття рекомендована до друку 02.09.2025 р.
Опубліковано 30.12.2025 р.

REFERENCES

1. Havryliuk, A. (2024). GDPR Ukrainian style: key aspects of Draft Law No. 8153 «On Personal Data Protection». Sayenko Kharenko. https://sk.ua/uk/gdpr-po-ukrainski-kljuchovi-aspekti-zp-8153-pro-zahist-personalnih-danih/ [in Ukrainian].

2. Hyliaka, O.S. (2023). The right to privacy and personal data protection in the context of digitalisation. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy, 30(1), 15–32.* https://doi.org/10.31359/1993-0909-2023-30-1-15 [in Ukrainian].

3. Dovhan, O.D. (Comp.). (2023). Cybersecurity in the information society: information and analytical digest (No. 10). Instytut informatsii, bezpeky i prava NAPrN Ukrainy; Natsionalna biblioteka Ukrainy im. V. I. Vernadskoho [in Ukrainian].

4. Dunaiev, I., & Luhovenko, N. (2025). The state and personal data in the post-GDPR world: towards global consensus or regulatory fragmentation? *Teoriia ta praktyka derzhavnoho upravlinnia, 2(79), 28–62.* https://doi.org/10.26565/1727-6667-2024-2-02 [in Ukrainian].

5. European Business Association. (2025). Discussion of Draft Law No. 8153 «On Personal Data Protection». URL: https://eba.com.ua/obgovorennya-zakonoproyektu-8153-pro-zahyst-personalnyh-danyh/ [in Ukrainian].

6. Zhakhalov, Ya. (2025). Ukraine reforms cyber defence after attack on registries. This will expand the powers of the State Special Communications Service. DOU. https://dou.ua/lenta/news/new-law-on-cybersecurity/ [in Ukrainian].

7. Report on the state of cyber protection of state information resources and critical infrastructure objects in 2023. (2024). Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy [in Ukrainian].

8. Kovaliv, M., Skrynkovskyi, R., Nazar, Yu., Yesimov, S., Krasnytskyi, I., Kaidrovych, Kh., Kniaz, S., & Kemska, Yu. (2021). Legal provision of cybersecurity of critical information infrastructure of Ukraine. *Path of Science, 7(4), 2011–2018.* https://doi.org/10.22178/pos.69-12 [in Ukrainian].

9. Udovenko, O.V., & Velychko, L.Yu. (2024). How does the «Brussels effect» shape new standards? The impact of the GDPR personal data protection standard and other EU initiatives on Ukraine and countries outside the European Union. *Aktualni problemy derzhavnoho upravlinnia, 2(65), 187–215.* https://doi.org/10.26565/1684-8489-2024-2-10 [in Ukrainian].

10. Furashev, V.M. (2012). Cyberspace and information space, cybersecurity and information security: essence, definitions, differences. *Informatsiia i pravo, 2, 162–169*. [in Ukrainian].

11. Annual report of the Ukrainian Parliament Commissioner for Human Rights on the state of observance and protection of human and citizens' rights and freedoms in Ukraine for 2024. (2025). Ofis Ombudsmana. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/1-eng-web.pdf [in Ukrainian].

12. Yarmolenko, O., & Husiev, H. (2025). The state reforms cyber defence after a large-scale breach. The State Special Communications Service will receive new powers – and this service is being criticised again. *Babel.* URL: https://babel.ua/texts/116673-derzhava-reformuye-kiberzahist-pislya-masshtabnogo-zlamu-derzhspeczv-yazku-otrimaye-novi-povnovazhennya-i-cyu-sluzhbu-znovu-kritikuyut-babel-poyasnyuye-sut-reformi-i-prosit-jiji-avtora-vidpovisti-na-k [in Ukrainian].

13. Bepon, K. (2024). 5 Questions (and Answers) About the Kyivstar Attack. *KELA Cyber*. URL: https://www.kelacyber.com/blog/5-questions-and-answers-about-the-kyivstar-attack/

14. CERT-UA recorded 4,315 cyber incidents in 2024. (2025). State Service of Special Communications and Information Protection of Ukraine. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

15. De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services. *Computer Law & Security Review, 34(2), 193–203.* https://doi.org/10.1016/j.clsr.2017.10.003

16. 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. (2022). *Official Journal of the European Union, L 333, 80–152*.

17. Due to Russia's cyberattack, all registration actions are unavailable, about 25 state registers suspended. (2024). *Interfax-Ukraine*. URL: https://en.interfax.com.ua/news/general/1036066.html

18. ENISA. (2024). Report on the State of Cybersecurity in the Union 2024. https://doi.org/10.2824/0401593

19. ENISA Threat Landscape 2024. (2024). European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

20. ENISA Threat Landscape 2025. (2025). European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

21. EU Cyber Resilience Act takes effect, brings new era of mandatory cybersecurity standards for digital products. (2024). Industrial Cyber. URL: https://industrialcyber.co/regulation-standards-and-compliance/eu-cyber-resilience-act-takes-effect-brings-new-era-of-mandatory-cybersecurity-standards-for-digital-products/

22. European Union Data Privacy: What's Next for 2025? (2025). TrustArc. URL: https://trustarc.com/resource/european-union-data-privacy-whats-next-for-2025/

23. Giannopoulos, G., Smith, H., & Theocharidou, M. (2023). The Landscape of Hybrid Threats: A Conceptual Model. *Publications Office of the European Union*.

24. Hybrid threats as a concept. (n.d.). Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats. URL: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

25. Investment Climate Statements 2025: Ukraine. (2025). U.S. Department of State. URL: https://www.state.gov/reports/2025-investment-climate-statements/ukraine

26. Kuner, C., Bygrave, L., & Docksey, C. (Eds.). (2020). The EU General Data Protection Regulation (GDPR): A Commentary. Oxford University Press.

27. Lynskey, O. (2015). The Foundations of EU Data Protection Law. Oxford University Press.

28. NIS 2 Directive, Article 23: Reporting obligations. (n.d.). URL: https://www.nis-2-directive.com/NIS_2_Directive_Article_23.html

29. Petkova, B. (2019). Privacy as Europe's First Amendment. *European Law Journal, 25(2), 140–154.* https://doi.org/10.1111/eulj.12316

30. Reisinger, T., Wagner, I., & Boiten, E. A. (2022). Security and Privacy in Unified Communication. *ACM Computing Surveys, 55(3), 1–35.* https://doi.org/10.1145/3498335

31. Rotenberg, M. (2020). Schrems II, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection. *European Law Journal, 26(1–2), 141–152*. https://doi.org/10.1111/eulj.12370

32. Russian Sandworm hackers breach Kyivstar network, causing devastating damage and signaling warning to the West. (2024). Industrial Cyber. URL: https://industrialcyber.co/threat-landscape/russian-sandworm-hackers-breach-kyivstar-network-causing-devastating-damage-and-signaling-warning-to-the-west/

33. Shastri, S., Wasserman, M., & Chidambaram, V. (2021). How Design and Operation of Modern Cloud-Scale Systems Conflict with GDPR. Proceedings of the 2021 ACM Symposium on Cloud Computing, 560–566.

34. The EU Critical Entities Resilience Directive – What is the impact on your organisation? (2024). Osborne Clarke. URL: https://www.osborneclarke.com/insights/eu-critical-entities-resilience-directive-what-impact-your-organisation

35. The NIS 2 Directive: Updates, Compliance, Training. (n.d.). URL: https://www.nis-2-directive.com/

36. Voss, W.G., & Houser, K. (2019). Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal, 56(2), 287–344*. https://doi.org/10.1111/ablj.12139

37. Weaponizing social Identities: What can we learn from examples of targeted disinformation? (2024). Hybrid CoE. URL: https://www.hybridcoe.fi/news/weaponizing-social-identities-what-can-we-learn-from-examples-of-targeted-disinformation/

38. Yeung, K., & Bygrave, L.A. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance, 16(1), 137–168*. https://doi.org/10.1111/rego.12401

The article was received by the editors 27.07.2025.
The article is recommended for printing 02.09.2025.
Published 30.12.2025.