УДК 004.056:342.9
DOI https://doi.org/10.32782/TNU-2707-0581/2026.2/10

Нікітін В. В.
https://orcid.org/0000-0001-6915-6319
Київський національний університет будівництва і архітектури

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПУБЛІЧНО-ПРАВОВІ Й ПРИВАТНО-ПРАВОВІ МЕХАНІЗМИ, ОБОВ'ЯЗКИ ОПЕРАТОРІВ, ВІДПОВІДАЛЬНІСТЬ ЗА ІНЦИДЕНТИ, ВЗАЄМОДІЯ ДЕРЖАВИ Й БІЗНЕСУ, СТРАХУВАННЯ КІБЕРРИЗИКІВ

У статті досліджено правову архітектоніку кібербезпеки та захисту критичної інфраструктури (КІ) як інституту подвійної природи – публічно-правової (державна політика, регуляторний нагляд, обов'язкові стандарти безпеки, обмін інформацією та реагування) і приватно-правової (договірні моделі, деліктна відповідальність, комплаєнс, страхування кіберризиків). На основі аналізу Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про критичну інфраструктуру», законодавства про захист персональних даних та цивільно-правових норм про відшкодування шкоди обґрунтовано систему обов'язків операторів/суб'єктів КІ: управління ризиками, організаційно-технічні заходи, безперервність функціонування, ведення журналів подій, взаємодія з CERT-UA/НКЦК та своєчасне повідомлення про кіберінциденти [1, с. 40], [2, с. 829].

Показано, що правова відповідальність за кіберінциденти має багаторівневий характер: адміністративну, кримінальну, цивільно-правову (договірну й позадоговірну), а також відповідальність держави за шкоду, спричинену незаконними рішеннями/діями органів влади у державно-приватних відносинах. Окрему увагу приділено відшкодуванню моральної шкоди за витік персональних даних, де застосовуються підходи Верховного Суду (зокрема Великої Палати) щодо критеріїв справедливості компенсації та доказування немайнових втрат. Розкрито потенціал кіберстрахування як приватно-правового інструменту перерозподілу ризиків, його обмеження (виключення, франшизи, умови про мінімальні контрольні заходи) та можливі стимули держави до розвитку ринку. Запропоновано напрями вдосконалення законодавства і практики: гармонізацію з підходами Директиви (ЄС) 2022/2555 (NIS2), уточнення режиму повідомлення про інциденти, визначення мінімальних кіберобов'язків для операторів КІ, посилення захисту персональних даних та процесуальних механізмів відшкодування шкоди.

Ключові слова: *кібербезпека, критична інфраструктура, кіберінцидент, оператор КІ, державно-приватне партнерство, деліктна відповідальність, кіберстрахування.*

Постановка проблеми. Критична інфраструктура (КІ) у сучасній державі є системоутворювальним комплексом об'єктів і сервісів, без яких неможливі базові соціально-економічні процеси: енергопостачання, транспорт, зв'язок, фінансові послуги, охорона здоров'я, водопостачання, державне управління тощо. Цифровізація цих сфер, з одного боку, підвищує ефективність, а з іншого – множить поверхню атак: промислові мережі (ICS/SCADA), хмарні сервіси, Інтернет речей, віддалені робочі місця. З огляду на воєнний стан і постійну активність державних та недержавних кіберзагроз, захист КІ перетворився з «питання техніки» на ключову функцію публічної влади і бізнесу [2, с. 828–829].

Українське право формує багаторівневий режим кіберзахисту, в якому взаємодіють конституційні гарантії безпеки та приватності, адміністративно-правові інструменти регуляції та контролю, цивільно-правові моделі відповідальності, а також спеціальні процедури виявлення, фіксації та реагування на кіберінциденти. Саме така «подвійна» природа інституту кібербезпеки КІ – поєднання імперативних обов'язків (public law) і диспозитивних/ризикорозподільчих механізмів (private law) – визначає його методологічну складність і практичну значущість [1, с. 35; 2, с. 829].

На практиці основні проблеми виникають на стику режимів: 1) коли оператор КІ формально

виконує публічно-правові вимоги, але несе приватно-правову відповідальність перед контрагентами/споживачами; 2) коли порушення спричиняє витік персональних даних і постає питання моральної шкоди; 3) коли інцидент пов'язаний із діями (бездіяльністю) державного органу – наприклад, регулятора, замовника у державно-приватному партнерстві або органу, що координує реагування. Ці ситуації вимагають доктринально й процесуально узгоджених підходів.

Актуальність теми зумовлена трьома групами факторів. По-перше, інтенсивністю кіберінцидентів у секторі державного управління та підприємств, що забезпечують життєдіяльність держави, а також зростанням впливу інцидентів на фізичну безпеку та економіку. По-друге, нормативною еволюцією: у 2021 році ухвалено Закон України «Про критичну інфраструктуру», який заклав базові інституційні рамки для класифікації об'єктів і визначення суб'єктів системи захисту, але значна частина механізмів реалізується через підзаконні акти і секторальні правила. По-третє, інтеграційним вектором України та необхідністю врахування європейських підходів до кіберобов'язків (зокрема NIS2), що передбачають ризик-орієнтоване управління, обов'язкове повідомлення про інциденти та ефективні санкції [1, с. 40].

Паралельно з публічно-правовим регулюванням стрімко розвивається приватноправовий сегмент: договори про надання хмарних послуг, аутсорсинг SOC/CSIRT, ліцензійні договори на програмне забезпечення, угоди про рівень сервісу (SLA), а також страхові продукти від кіберризиків. У цих договорах фіксуються стандарти належної обачності, розподіляються ризики простою, втрати даних та відповідальності перед третіми особами. Відсутність єдиного методологічного «містка» між публічним і приватним правом породжує колізії у кваліфікації порушень та доказуванні збитків.

Аналіз останніх досліджень і публікацій. Питання кібербезпеки у правовому вимірі досліджуються українськими науковцями різних шкіл: у площині інформаційного права, адміністративного права та національної безпеки. Зокрема, Б. В. Богдан аналізує державну політику захисту КІ в умовах воєнного стану, підкреслюючи особливості нормативних режимів та інституційної координації [2, с. 828–829]. В. Богом'я та В. Галунько розглядають правове регулювання кібербезпеки критичної інфраструктури з урахуванням категорій «кіберінцидент», «кіберзагроза» та порівняльних підходів ЄС [1, с. 37–38, 40].

У ширшому науковому контексті варто відзначити праці представників української школи інформаційного права. Так, О. А. Баранов у дослідженнях щодо правового регулювання цифрових технологій (зокрема Інтернету речей) окреслює системні ризики та потребу адаптації традиційних інститутів відповідальності до цифрового середовища [3, с. 30–35]. В. М. Фурашев у працях з інформаційної безпеки та правових питань ІТ-розвитку акцентує на необхідності комплексного нормативного підходу до захисту інформаційних ресурсів [4, с. 12–18]. Окремий пласт складають міжгалузеві дослідження страхування кіберризиків, які пропонують моделі покриття кібервідповідальності та майнових втрат [5, с. 44–50].

Водночас у вітчизняній доктрині залишається недостатньо опрацьованою проблема «зшивки» публічно-правового режиму кіберобов'язків операторів КІ з приватно-правовими наслідками інцидентів: відшкодуванням збитків контрагентам, моральної шкоди за витік персональних даних, регресом між учасниками ланцюга постачання, а також із відповідальністю держави у державно-приватних відносинах. Ця стаття спрямована на заповнення зазначеної прогалини.

Постановка завдання. Метою статті є комплексне висвітлення публічно-правових і приватно-правових механізмів кібербезпеки та захисту критичної інфраструктури, визначення обов'язків операторів КІ та моделей відповідальності за кіберінциденти, а також обґрунтування напрямів удосконалення законодавства та практики взаємодії держави й бізнесу.

Для досягнення мети поставлено такі завдання: 1) окреслити понятійно-категоріальну основу та систему суб'єктів у сфері кіберзахисту КІ; 2) систематизувати публічно-правові інструменти (стандарти, нагляд, реагування, санкції) та їх інституційне забезпечення; 3) розкрити приватно-правові механізми (договори, комплаєнс, делікт, страхування) і типові розподіли ризиків; 4) проаналізувати відповідальність операторів за інциденти, включно з моральною шкодою від витоків даних; 5) дослідити відповідальність у державно-приватних відносинах та підходи Великої Палати Верховного Суду; 6) сформулювати пропозиції щодо гармонізації українського підходу з європейськими стандартами та підвищення ефективності практики.

Виклад основного матеріалу. Українське законодавство використовує взаємопов'язані категорії «критична інфраструктура», «критична інформаційна інфраструктура», «кібербезпека»,

«кіберзагроза» та «кіберінцидент». Закон України «Про критичну інфраструктуру» визначає загальну систему ідентифікації та категоризації об'єктів, суб'єктів системи захисту та принципи функціонування у мирний час, тоді як особливості в умовах надзвичайного стану й воєнного стану деталізуються іншими актами, що підкреслюється у доктрині [2, с. 829].

Закон України «Про основні засади забезпечення кібербезпеки України» закріплює базові принципи кіберзахисту, суб'єктів національної системи та поняття «кіберінцидент» як порушення нормального функціонування інформаційно-телекомунікаційних систем або доступності/цілісності даних [1, с. 38]. Юридична техніка цих дефініцій має практичне значення, адже впливає на обсяг обов'язку повідомляти про інцидент, межі кримінально-правової кваліфікації, а також на страхові умови щодо настання «страхового випадку».

Системність регулювання забезпечують також норми цивільного та господарського законодавства про відповідальність за невиконання зобов'язань і завдання шкоди, законодавство про інформацію та персональні дані, а також підзаконні акти, що встановлюють вимоги до організаційно-технічних заходів, аудиту та обміну інформацією про кіберзагрози.

Публічно-правові механізми: політика, нагляд, координація, санкції. Публічно-правовий сегмент кібербезпеки КІ охоплює: (а) формування державної політики та стратегічних пріоритетів; (б) визначення обов'язкових правил/мінімальних стандартів безпеки; (в) інституційну координацію реагування на інциденти; (г) контроль і застосування санкцій. У період воєнного стану ця система доповнюється спеціальними режимами захисту об'єктів та процедурою реагування на кризові ситуації [2, с. 829].

Функціонально важливо розрізняти регуляторний контроль (перевірки, припис, штраф) і координаційно-оперативні механізми (CERT/CSIRT, розслідування інцидентів, обмін IOC, сповіщення щодо вразливостей). Ефективність публічно-правового впливу значною мірою залежить від побудови довіри між державними органами й операторами КІ, оскільки без «добровільного комплаєнсу» та своєчасного повідомлення про інциденти реакція держави стає запізнілою. Саме тому порівняльний досвід ЄС (NIS2) закріплює поєднання ризик-менеджменту, обов'язку реагування та нагляду/санкцій [1, с. 40].

Окремою публічно-правовою площиною виступає державний нагляд за захистом персональних даних. У контексті КІ витоки персональних даних можуть супроводжувати фактичні збої надання послуг (наприклад, у транспорті, енергетиці чи фінансових сервісах), а отже порушують не лише «інформаційні», але й базові соціальні права. Це вимагає синхронізації кіберрегулювання та режиму персональних даних: інцидент-репортинг, повідомлення суб'єктів даних, оцінка впливу та відновлення.

Приватно-правові механізми: договори, комплаєнс, відповідальність і доказування. Приватно-правова складова кібербезпеки КІ реалізується насамперед через договори. Типові моделі включають: (1) договори постачання/обслуговування обладнання (у т.ч. промислових контролерів); (2) ліцензійні договори та договори підтримки ПЗ; (3) договори з провайдерами хмарної інфраструктури та центрами обробки даних; (4) аутсорсинг кіберзахисту (SOC/CSIRT); (5) договори про рівень сервісу (SLA), що встановлюють показники доступності та час відновлення. Через такі договори формується «приватний стандарт належної кіберобачності», який може бути як жорсткішим, так і м'якшим за мінімальні публічно-правові вимоги.

Особливість приватноправового режиму – необхідність доказування причинно-наслідкового зв'язку між порушенням кіберобов'язків та збитками. Для КІ це складно, адже інциденти часто мають багатофакторну природу (ланцюг постачання, нульовий день, людський фактор, збої електропостачання). Доктрина деліктного права вказує, що проста послідовність подій не є достатньою для встановлення причинного зв'язку; потрібна необхідність і закономірність наслідків [6, с. 125–128].

Тому у договірній практиці поширені: гарантійні положення про мінімальні заходи безпеки (MFA, резервне копіювання, сегментація мереж), обов'язок повідомляти про інцидент протягом визначеного часу, а також договірні обмеження відповідальності (ліміти, виключення непрямих збитків). Однак у відносинах із споживачами/фізичними особами такі обмеження можуть бути обмежені імперативними нормами про захист прав споживачів та відшкодування моральної шкоди.

Обов'язки операторів/суб'єктів КІ: зміст і стандарти належності. Систему ключових обов'язків операторів КІ доцільно групувати у чотири блоки: (а) управління ризиками і планування; (б) організаційні й технічні заходи (політики доступу, сегментація, криптографічний

захист, контроль змін); (в) безперервність та відновлення (BCP/DRP, резервні копії, тестування); (г) взаємодія та повідомлення про інциденти (комунікаційні протоколи, передача інформації до компетентних органів, збереження доказів). У науковій літературі підкреслюється, що повідомлення про кіберінциденти є інструментом швидкого реагування та обміну даними про загрози [1, с. 40].

У період воєнного стану додаткового значення набувають режими фізичного захисту та резервування критичних процесів, включно з розподіленими центрами керування, альтернативними каналами зв'язку та впровадженням кризового менеджменту [2, с. 829].

З позицій приватного права виконання цих обов'язків стає елементом доказування належної поведінки (due diligence). Оператор, який доведе, що впровадив мінімально необхідні заходи, може зменшити ризики деліктної відповідальності або розширити страхове покриття. Натомість невиконання базових кіберконтролів часто кваліфікується як груба необережність, що тягне відмову у виплаті страхового відшкодування або регрес страховика.

Відповідальність за кіберінциденти: договірна, деліктна, адміністративна та кримінальна. Юридична відповідальність у сфері кіберінцидентів є багаторівневою. Публічно-правова відповідальність реалізується через адміністративні санкції (за порушення вимог безпеки, порядку обробки даних, невиконання приписів регулятора) та кримінальну відповідальність за втручання в роботу інформаційних систем, несанкціоноване поширення інформації, шкідливе програмне забезпечення тощо. Приватно-правова відповідальність реалізується через договірні санкції (неустойка, штраф, відшкодування збитків) та делікт (відшкодування шкоди, моральної шкоди, компенсація витрат на відновлення).

Для КІ ключовим є поєднання двох площин порушення: 1) порушення обов'язків перед державою (публічно-правові обов'язки щодо забезпечення безпеки та інцидент-репортингу), 2) порушення обов'язків перед контрагентами та споживачами (доступність послуг, конфіденційність даних, цілісність). На стику цих площин виникає проблема кваліфікації інциденту і «вибору відповідальності», а також процесуальної юрисдикції.

Моральна шкода за витік персональних даних: підходи Верховного Суду та Велика Палата. Витік персональних даних у результаті кіберінциденту може спричиняти не лише майнові втрати (шахрайство, викрадення коштів), а й немайнові (моральні) страждання: відчуття небезпеки, порушення приватності, репутаційні втрати, психологічний дискомфорт. Цивільно-правовою основою є ст. 23 ЦК України, яка допускає компенсацію моральної шкоди внаслідок порушення особистих немайнових прав, а також норми Закону України «Про захист персональних даних», що встановлює принципи обробки даних та право суб'єкта на захист.

Важливою є судова практика Великої Палати Верховного Суду щодо критеріїв визначення розміру моральної шкоди. Так, у постанові від 12.11.2019 у справі № 904/4494/18 Велика Палата вказала, що розмір компенсації залежить від характеру діяння порушника, негативних наслідків для позивача та має ґрунтуватися на вимогах розумності та справедливості [7, с. 15–17]. Ці підходи релевантні для оцінки моральної шкоди від витоку даних: ступінь втручання в приватність, масштаб поширення даних, вразливість категорій даних (наприклад, медичні, фінансові), наявність подальших наслідків (шахрайство, переслідування).

Додатково, у постанові ВП ВС від 15.12.2020 у справі № 752/17832/14-ц Велика Палата аналізувала механізми компенсації моральної шкоди, завданої незаконними діями органів державної влади, підкреслюючи необхідність врахування тривалості порушення і реальних наслідків для особи (психологічні страждання, порушення звичного способу життя) [8, с. 80–82]. Хоча фабула справи не стосувалася кіберінцидентів, правові підходи до оцінки немайнових втрат можуть бути застосовані і до витоків даних, особливо коли інцидент пов'язаний із неналежною діяльністю суб'єкта публічної влади або комунального оператора.

Суди касаційних інстанцій також розвивають практику безпосередньо щодо втручання у приватність: наприклад, у постанові Касаційного цивільного суду ВС від 19.07.2023 у справі № 214/11028/21 зазначено, що непропорційне втручання у приватне життя здатне спричинити моральні страждання, які підлягають компенсації [9, с. 6-8]. Для спорів про витік даних це означає, що доказування може будуватися не лише на економічних наслідках, а й на доведенні самого факту істотного порушення приватності та почуття небезпеки.

Відповідальність у державно-приватних відносинах: позиції Великої Палати. У сфері КІ

значна частина взаємодії держави і бізнесу відбувається в режимі державних контрактів, концесій, державно-приватного партнерства (ДПП), регуляторного нагляду та адміністративних дозволів. У разі кіберінциденту постає питання: хто і в якому порядку відповідає за шкоду – оператор, постачальник або держава (регулятор/координатор).

Показовою є позиція Великої Палати Верховного Суду у справі № 925/556/21 (01.03.2023), яка підтверджує подвійність обов'язків: реєстрація податкової накладної є публічно-правовим обов'язком, але сторони господарського договору можуть встановлювати договірний обов'язок надати належно зареєстрований документ, порушення якого може завдати збитків [10, с. 69–75]. Водночас, якщо збитки є наслідком незаконних дій податкового органу, вони підлягають відшкодуванню не в договірних, а в позадоговірних відносинах за рахунок держави (ст. 56 Конституції, статті 1173-1174 ЦК) [10, с. 101–137].

Цей висновок має принципове значення для кіберінцидентів у КІ. По-перше, він дозволяє правильно розмежувати ризики: оператор відповідає перед контрагентом за невиконання SLA/зобов'язань щодо безпеки, але може мати підстави для регресу чи окремого позову до держави, якщо шкода є наслідком незаконного владного рішення (наприклад, протиправних обмежень доступу до інфраструктури або неналежних координаційних дій). По-друге, підкреслюється значення належної поведінки оператора: для доведення державної відповідальності необхідно встановити протиправність акта/дії органу, факт шкоди та причинний зв'язок [10, с. 138–159].

Взаємодія держави й бізнесу: інформаційний обмін, ДПП, стандарти реагування. Взаємодія держави й бізнесу у сфері кіберзахисту КІ має відбуватися за моделлю «спільної відповідальності» (shared responsibility). Держава визначає правила та координує реагування, а оператори впроваджують контрзаходи і надають інформацію про інциденти і вразливості. Наукові джерела підкреслюють, що зобов'язання повідомляти про інциденти підвищує швидкість реагування та ефективність обміну інформацією [1, с. 40].

У договірних моделях ДПП доцільно передбачати «кібердодатки» (cyber annex) з чіткими метриками безпеки, порядком аудиту та проведення пентестів, процедурою інцидент-комунікацій і розподілом витрат на відновлення. У воєнний час особливу роль відіграють кризові процедури та резервні сценарії функціонування [2, с. 828].

Інституційно важливо формувати секторальні центри обміну інформацією (ISAC) та протоколи розкриття вразливостей (coordinated vulnerability disclosure). Такі механізми зменшують «інформаційний розрив» між державою і ринком та впливають на доведення належної обачності (виконання best practices).

Страхування кіберризиків: приватно-правова відповідь на системні загрози. Кіберстрахування виконує функцію перерозподілу ризиків і стимулювання комплаєнсу. У теорії та практиці виділяють принаймні два підходи до покриття: (1) страхування кібервідповідальності (claims from third parties for data breaches, privacy violations), і (2) майнове страхування наслідків кібератак (business interruption, incident response costs) [5, с. 134–140].

Для операторів КІ страхування може бути особливо цінним через високу вартість простою та відновлення систем. Однак страхові продукти мають типові обмеження: виключення щодо державних актів війни/кібервійни, санкційних режимів, грубої необережності страхувальника, а також вимоги до мінімальних контрольних заходів (MFA, патч-менеджмент, бекапи).

Публічна влада може стимулювати ринок кіберстрахування не лише через обов'язковість, а через економічні стимули: податкові пільги для впровадження сертифікованих заходів безпеки, державні гарантії на катастрофічні кіберризики (stop-loss), а також розвиток стандартів оцінки кіберризиків і актуарних моделей. Такий підхід узгоджується з концепцією спільної відповідальності та підвищує стійкість КІ.

Внесок цієї наукової статті полягає у: (1) систематизації кібербезпеки та захисту критичної інфраструктури як інституту подвійної (публічно- та приватно-правової) природи; (2) побудові узгодженої моделі обов'язків операторів КІ, що поєднує імперативні вимоги держави та критерії належної обачності у приватноправових відносинах; (3) виокремленні двох «вузлів» правозастосування – моральної шкоди за витік даних та відповідальності у державно-приватних відносинах – із прив'язкою до позицій Великої Палати Верховного Суду; (4) формулюванні прикладних пропозицій щодо гармонізації українського режиму з підходами NIS2 і розвитку кіберстрахування як ринкового інструменту стійкості.

Практика реагування на кіберінциденти показує, що формальне виконання вимог закону без зрозумілої системи внутрішнього контролю не забезпечує реальної стійкості КІ. Тому приватно-

правовий вимір обов'язків операторів має спиратися на комплаєнс-програми, які одночасно є доказом належної обачності у договірних та деліктних спорах (due diligence).

У комплаєнс-моделі доцільно розрізняти: (а) обов'язковий мінімум (імперативні вимоги щодо управління ризиками, реагування та повідомлення); (б) підвищені практики для «суттєвих/важливих» суб'єктів КІ; (в) добровільні стандарти, що підвищують довіру контрагентів і страхувальників. Для порівняння, Директива (ЄС) 2022/2555 (NIS2) прямо формулює вимоги до управління ризиками, реагування та звітування про інциденти, а також нагляд і санкції за їх невиконання [1, с. 40].

З практичної точки зору, системи управління інформаційною безпекою на основі ISO/IEC 27001 та галузевих профілів (NIST CSF, IEC 62443 для промислових систем) можуть бути використані як «міст» між технічними стандартами і юридичними критеріями належної поведінки. У договорах (постачання, аутсорсинг, хмарні послуги, обробка даних) це трансформується в конкретні SLA/OLA, вимоги до шифрування, резервного копіювання, журналювання, тестування на проникнення та порядку взаємодії при інциденті.

Аудит і тестування мають подвійне значення. По-перше, вони забезпечують виконання публічно-правових обов'язків щодо безперервності функціонування та захисту КІ. По-друге, вони знижують приватно-правові ризики: у спорах про відшкодування шкоди оператор може доводити, що вжив «усіх залежних від нього заходів» для недопущення шкоди, що кореспондує загальним підходам цивільної відповідальності (ст. 614 ЦК України) та відповідальності суб'єктів господарювання (ст. 614 ЦК України) [14].

Суттєвим є й питання ланцюгів постачання (supply chain). Для операторів КІ типовими є залежності від провайдерів електронних комунікацій, дата-центрів, постачальників SCADA/ICS, а також від підрядників, які мають доступ до критичних сегментів мережі. Звідси випливає вимога до законодавця: деталізувати мінімальні умови «кібер-угод» (кіберзастереження у договорах), включно з правом на аудит, обов'язком повідомляти про інциденти у визначені строки, та відповідальністю за порушення вимог безпеки.

Отже, комплаєнс і стандартизація мають розглядатися не як факультативна «добра практика», а як структурний елемент приватно-правової частини інституту кіберзахисту КІ, який забезпечує передбачуваність для бізнесу, страхового ринку та судового захисту прав потерпілих.

Висновки. Кібербезпека та захист КІ є інститутом подвійної природи: публічно-правові механізми встановлюють обов'язкові правила та координацію, а приватно-правові механізми розподіляють ризики і забезпечують відшкодування шкоди. Нормативна база України є сформованою на рівні рамкових законів, але потребує подальшої гармонізації з європейськими підходами (NIS2) та уточнення підзаконних процедур [1, с. 40].

Обов'язки операторів КІ доцільно закріпити у вигляді мінімального «профілю кіберстійкості» для основних секторів (енергія, транспорт, зв'язок, фінанси). Пропонується: (а) встановити єдині строки повідомлення про значні кіберінциденти та критерії «значності»; (b) нормативно передбачити обов'язок збереження цифрових доказів та проведення постінцидентного аналізу; (с) впровадити обов'язок регулярних оцінок ризику та аудиту контролів.

У приватно-правовій площині потрібно уніфікувати підходи до доказування збитків і причинного зв'язку у спорах про кіберінциденти: розробити методичні рекомендації щодо оцінки простоїв, вартості відновлення, втрати даних та репутаційних втрат, з урахуванням доктрини деліктного права [6, с. 125–128].

Блок моральної шкоди за витік даних потребує подальшої уніфікації судової практики. Доцільно на рівні узагальнень Верховного Суду роз'яснити стандарти доказування немайнових втрат у справах про витоки персональних даних, спираючись на критерії розумності й справедливості Великої Палати [7, с. 15–17]. Законодавчо доцільно передбачити можливість компенсації моральної шкоди за сам факт істотного порушення приватності (для чутливих категорій даних), що зменшить процесуальні бар'єри для потерпілих.

Відповідальність у державно-приватних відносинах потребує чіткого розмежування договірної та позадоговірної шкоди. Позиція Великої Палати у справі № 925/556/21 підказує принцип: якщо втрати зумовлені незаконними діями органу влади, шкода відшкодовується державою у деліктному порядку за ст. 1173–1174 ЦК [10, с. 101–146]. Для КІ це означає необхідність закріпити прозорі процедури оскарження координаційних рішень і механізми відшкодування шкоди операторам у разі протиправних втручань.

Ринок кіберстрахування потребує підтримки через стандартизацію оцінки ризиків та меха-

нізми публічно-приватної взаємодії. Доцільно розглянути введення обов'язкового страхування для окремих класів операторів КІ (за аналогією страхування відповідальності), але лише після розробки базових кіберстандартів і актуарних моделей [5, с. 134–140].

Для ефективного відшкодування моральної шкоди за витік даних доцільно передбачити процесуальні презумпції щодо факту немайнових страждань при доведеному порушенні режиму персональних даних та запровадити інструменти колективного захисту (групові позови/представницькі позови), що відповідає європейському підходу до захисту прав споживачів і суб'єктів даних.

У державно-приватних відносинах, пов'язаних із КІ (ліцензування, дозвільні процедури, контроль, блокування/обмеження доступу), потрібно закріпити обов'язок органів влади дотримуватися адміністративних процедур і стандартів належного урядування, а у випадку незаконних рішень – забезпечити швидке та повне відшкодування збитків бізнесу за правилами статей 1173–1174 ЦК України з урахуванням підходів Великої Палати Верховного Суду, розкритих у справі № 925/556/21 [10].

Список літератури:

1. Богом'я В., Галунько В. Правове регулювання кібербезпеки критичної інфраструктури в Україні. *Information Technology: Computer Science, Software Engineering and Cyber Security.* 2024. Вип. 4. С. 35–42. DOI https://doi.org/10.32782/IT/2024-4-5

2. Богдан Б. В. Державна політика у сфері захисту критичної інфраструктури під час дії воєнного стану. *Юридичний науковий електронний журнал*. 2025. № 1. С. 828–830. DOI https://doi.org/10.32782/2524-0374/2025-1/199.

3. Баранов О. А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання. Київ: Видавничий дім Дмитра Бураго, 2018. 224 с.

4. Фурашев В. М. Інформаційна безпека: правові аспекти (вибрані праці). Київ: [вид-во], 2019.

5. Р. В. Пікус, Ю. Л. Бабенко, Кібестрахування: нові можливості для страхового ринку України. *Економіка та держава*. 2022. № 2. С. 134–140. DOI: 10.32702/2306-6806.2022.2.134.

6. Отраднова О. О. Проблеми вдосконалення механізму цивільно-правового регулювання деліктних зобов'язань: монографія. Київ: Юрінком Інтер, 2014. 320 с.

7. Постанова Великої Палати Верховного Суду від 12.11.2019 у справі № 904/4494/18 (ЄДРСР 86035198).

8. Постанова Великої Палати Верховного Суду від 15.12.2020 у справі № 752/17832/14-ц.

9. Постанова Верховного Суду (Касаційний цивільний суд) від 19.07.2023 у справі № 214/11028/21.

10. Науковий висновок щодо справи № 925/556/21 (Велика Палата Верховного Суду). 2023. 7 с.

11. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

12. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

13. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

14. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.

Nikitin V. V. CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION: PUBLIC-LAW AND PRIVATE-LAW MECHANISMS, OPERATOR DUTIES, INCIDENT LIABILITY, STATE–BUSINESS COOPERATION, CYBER-RISK INSURANCE

The article examines the legal architecture of cybersecurity and critical infrastructure (CI) protection as a dual-nature institution combining public-law mechanisms (state policy, regulatory supervision, mandatory security standards, information sharing and incident response) and private-law mechanisms (contractual models, tort liability, compliance and cyber-risk insurance). Based on Ukrainian cybersecurity and CI legislation, personal data protection rules and civil-law provisions on damages, the paper substantiates a system of duties for CI operators/entities: risk management, organisational and technical safeguards, business continuity, logging, cooperation with CERT-UA/NCSCC and timely incident notification [1, p. 40], [2, p. 829].

It is argued that liability for cyber incidents is multi-layered, encompassing administrative, criminal and civil remedies (contractual and non-contractual), as well as state liability for damages caused by unlawful acts/decisions of public authorities in public–private relationships. A special focus is placed on compensation for non-pecuniary (moral) damage stemming from personal data leaks, where the Supreme Court's case-law

(including the Grand Chamber) provides key criteria of fairness, proportionality and evidentiary standards. The paper also analyses cyber insurance as a private governance tool for risk transfer, outlining typical coverage limitations (exclusions, deductibles, minimum-security warranties) and potential public incentives to foster the market. The author proposes legislative and practical improvements: further alignment with the EU NIS2 approach, clarification of incident reporting regimes, specification of baseline cybersecurity duties for CI operators, strengthening personal data safeguards and enhancing procedural routes for effective damage recovery.

Keywords: *cybersecurity, critical infrastructure, cyber incident, CI operator, public–private partnership, tort liability, cyber insurance.*

Дата першого надходження статті до видання: 16.02.2026
Дата прийняття статті до друку після рецензування: 18.03.2026
Дата публікації (оприлюднення) статті: 11.05.2026