НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет цивільної та господарської юстиції
Кафедра приватного права
Кафедра права інтелектуальної власності та патентної юстиції

ІТ-ПРАВО, КІБЕРБЕЗПЕКА ТА ШІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

МАТЕРІАЛИ
Всеукраїнської наукової конференції

28 березня 2026 р.

Одеса
Фенікс
2026

УДК 342.95:343.32 (477):351.863
І-92

За загальною редакцією
доктора юридичних наук, професора **Є. О. Харитонова**,
докторки юридичних наук, професорки **І. В. Давидової**

Упорядники-укладачі:

Давидова І. В. – доктор юридичних наук, професор, професор кафедри приватного права Національного університету «Одеська юридична академія»;

Калітенко О. М. – кандидат юридичних наук, доцент, професор кафедри приватного права Національного університету «Одеська юридична академія»;

Бобейко Н. І. – лаборантка кафедри приватного права Національного університету «Одеська юридична академія».

І-92 **ІТ-право, кібербезпека та ШІ в умовах гібридної війни** : мате-ріали Всеукр. наук. конф. (Одеса, 28 берез. 2026 р.) / за заг. ред.: д-ра юрид. наук, проф. Є. О. Харитонова, д-ра юрид наук, проф. І. В. Давидової. Одеса : Фенікс, 2026. 300 с. DOI: https://doi.org/10.32837/11300.33701

ISBN 978-617-8763-22-0

Збірник містить матеріали доповідей, присвячені актуальним проблемам ІТ-права, кібербезпеки, цифрової трансформації суспільних відносин, правового регулювання штучного інтелекту та захисту інформації в умовах гібридної війни, які були оприлюднені на Всеукраїнській науковій конференції 26 березня 2026 року в Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення науковців, викладачів, здобувачів освіти, практикуючих юристів, фахівців у сфері інформаційних технологій і кібербезпеки з результатами сучасних досліджень щодо правових, організаційних і технологічних аспектів функціонування цифрового середовища в умовах сучасних викликів. Матеріали видання можуть бути використані в науковій, освітній і практичній діяльності, а також під час подальшого вдосконалення правового регулювання цифрових відносин і забезпечення кібербезпеки України.

342.95 : 343.32 (477) : 351.863

Матеріали видано за авторською редакцією.
Повну відповідальність за достовірність і якість поданого матеріалу несуть учасники Всеукраїнської наукової конференції, їхні наукові керівники, рецензенти і структурні підрозділи вищих навчальних закладів та установ, які рекомендували ці матеріали до друку.

ISBN 978-617-8763-22-0

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ
Всеукраїнської наукової конференції

Харитонов Є. О. – завідувач кафедри приватного права Національного університету «Одеська юридична академія», д-р юрид. наук, проф. (голова);

Федотов О. П. – начальник науково- дослідної частини, професор кафедри морського, митного та інформаційного права, д-р юрид. наук, проф. (заступник голови);

Харитонова О. І. – завідувачка кафедри права інтелектуальної власності і патентної юстиції, д-р юрид. наук, проф.;

Галупова Л. І. – доцентка кафедри права інтелектуальної власності і патентної юстиції, канд. юрид. наук, доц.;

Зубар В. М. – професор кафедри приватного права, канд. юрид. наук, проф.;

Калітенко О. М. – професорка кафедри приватного права, канд. юрид. наук, доц.;

Кривенко Ю. В. – доцентка кафедри приватного права, канд.юрид. наук, доц.;

Токарева В. О. – доцентка кафедри приватного права, д-р юрид. наук,доц.;

Бобейко Н. І. – лаборантка кафедри приватного права.

. ,

рот, захистивши при цьому інтереси особи. І тим самим система речових прав має бути доповнена нормами про володіння та розпорядження анатомічними матеріалами, що базуються на принципі некомерційності (альтруїзму) та інформованої згоди.

Вовчок Руслан Володимирович
аспірант кафедри приватного права
Національного університету «Одеська юридична академія»

КІБЕРІНЦИДЕНТИ ЯК ОБСТАВИНИ НЕПЕРЕБОРНОЇ СИЛИ В ІТ-ДОГОВОРАХ

Кіберінцидент як підстава звільнення від відповідальності за порушення договірного зобов'язання є одним із найбільш дискусійних і методологічно не вирішених питань сучасного договірного права. Масштабні кібератаки – NotPetya (2017), атака на Colonial Pipeline (2021), інциденти з SolarWinds і Log4j, а також систематичні атаки на критичну інфраструктуру України після 24 лютого 2022 року – переконливо продемонстрували: кіберінцидент здатний паралізувати виконання договірних зобов'язань у спосіб, не менш руйнівний, ніж фізична катастрофа або збройний конфлікт [1, с. 117]. Однак, на відміну від повені, землетрусу або воєнних дій, кіберінцидент є явищем, чия правова кваліфікація як «обставини непереборної сили» у розумінні статті 617 ЦК України і відповідних договірних застережень залишається предметом гострої доктринальної дискусії і непослідовної судової практики. Центральна проблема полягає у принциповій відмінності кіберінциденту від класичних форс-мажорних обставин: він може бути прогнозованим, може бути наслідком недостатньої технічної захищеності сторони-порушника, може бути організований конкурентом або третьою особою – і у кожному з цих випадків відповідь на питання «чи є кіберінцидент форс-мажором?» має бути принципово різною.

Доктрина форс-мажору – непереборної сили як підстави звільнення від відповідальності за порушення зобов'язання – є однією з найбільш стійких конструкцій цивільного права, що бере

початок ще від римського принципу «casus a nullo praestantur». Стаття 617 ЦК України відтворює класичні ознаки непереборної сили: надзвичайність (виняткова, непередбачувана подія), невідворотність (неможливість запобігти наслідкам за будь-яких умов) і об'єктивність (незалежність від волі сторони-боржника). Торгово-промислова палата України уповноважена засвідчувати обставини форс-мажору, що надає процесуального значення факту настання таких обставин у договірних спорах.

Проте класична доктрина формувалась для природних і соціальних катастроф, де всі три ознаки є самоочевидними: землетрус є надзвичайним, невідворотним і об'єктивним явищем за визначенням. Кіберінцидент порушує цю тріаду в усіх трьох вимірах одночасно: він може бути частково передбачуваним через оцінку вразливостей; його наслідки можуть бути мінімізовані або навіть відвернуті належними заходами кіберзахисту; і він нерідко є продуктом дій людини – хакера, конкурента або іноземної спецслужби, – що розмиває «об'єктивність» події. Саме ця тріада методологічних проблем робить правову кваліфікацію кіберінцидентів нетривіальним завданням.

Методологічно вирішальним кроком у правовій кваліфікації кіберінцидентів як форс-мажору є побудова диференційованої класифікації за сукупністю критеріїв, що визначають юридичну природу конкретного інциденту. Доречним є, на нашу думку, запропонувати чотири категорії кіберінцидентів за критерієм форс-мажорності. По-перше, масштабні атаки державного або квазідержавного рівня (nation-state attacks) – на зразок NotPetya або атак на КІАС у 2022 році, – що мають ознаки воєнної операції і завдають шкоди незалежно від рівня захищеності жертви: такі інциденти найбільш відповідають критеріям форс-мажору і мають кваліфікуватись як такі за наявності зв'язку між загальним геополітичним контекстом і конкретним порушенням зобов'язання. По-друге, масові автоматизовані атаки (ransomware, DDoS-кампанії), що вражають тисячі суб'єктів одночасно незалежно від їхнього рівня захисту: їх кваліфікація як форс-мажору є обґрунтованою

лише за умови, що сторона-боржник вжила розумних заходів кіберзахисту відповідно до галузевих стандартів. По-третє, цільові атаки на конкретну організацію (targeted attacks, APT): їх форс-мажорна кваліфікація є найбільш сумнівною, оскільки адресний характер атаки свідчить про наявність конкретного ризику, управління яким є прямим обов'язком суб'єкта. По-четверте, не можуть визнаватися форс-мажорними обставинами інциденти, що стали наслідком експлуатації відомих вразливостей програмного забезпечення, якщо відповідна сторона мала можливість своєчасно усунути такі вразливості або вжити необхідних заходів захисту, але не зробила цього.

Центральним правовим питанням при оцінці кіберінциденту як форс-мажорної обставини є встановлення того, чи вжила сторона-боржник усіх розумно очікуваних заходів для запобігання інциденту або мінімізації його наслідків. За своєю суттю цей критерій є функціональним аналогом стандарту належної обачності, традиційно застосовуваного у цивільному праві, однак у сфері цифрових відносин він потребує конкретизації з урахуванням сучасних технічних та організаційних вимог кібербезпеки.

Правова наука і судова практика починають формувати контури цього стандарту: він включає відповідність кращим галузевим практикам кіберзахисту (ISO/IEC 27001, NIST Cybersecurity Framework, відповідні стандарти SOC 2), наявність і реалізацію плану реагування на інциденти (Incident Response Plan), регулярне оновлення програмного забезпечення і усунення відомих вразливостей, а також сегментацію мережі і резервне копіювання критичних даних. Відсутність будь-якого з цих елементів є підставою для висновку про те, що сторона не вжила розумних заходів і тому не може посилатись на форс-мажорний характер інциденту [2, с.276]. Практично важливим є питання про те, чи має цей стандарт бути закріплений у самому IT-договорі через спеціальне кіберзастереження, чи він застосовується незалежно від договірного регулювання як об'єктивний правовий критерій: порівняльний аналіз свідчить на користь гібридного підходу – стандарт існує

об'єктивно, але договірне кіберзастереження може конкретизувати і підвищити його рівень для конкретних відносин [3].

Практика розгляду спорів, пов'язаних із кіберінцидентами як підставою форс-мажору, є поки що обмеженою, але надзвичайно показовою. Найрезонанснішим і доктринально значущим є судовий процес у справі Merck & Co. v. Ace American Insurance Co. (Верховний суд Нью-Джерсі, 2023) у зв'язку з атакою NotPetya: страховик спочатку відмовив у відшкодуванні збитків на суму 1,4 млрд доларів, посилаючись на застереження про «воєнні дії» у страховому полісі, однак суд вирішив спір на користь позивача, вказавши, що застереження про воєнні дії вимагає оголошеного чи формально визнаного збройного конфлікту і не охоплює автоматично кібератаки державного рівня [4]. В Україні ТПП видавала сертифікати форс-мажору у зв'язку із кібератаками на державні інформаційні системи і критичну інфраструктуру після 24 лютого 2022 року, однак критерії, за якими конкретний кіберінцидент визнається форс-мажором, залишаються непублічними і непрозорими. Вітчизняна судова практика у цій сфері є мінімальною і непослідовною, що у поєднанні із зростаючою кількістю IT-договорів і кіберінцидентів утворює системну прогалину правозастосування.

У відсутність достатньої законодавчої і судової визначеності щодо правового режиму кіберінцидентів у IT-договорах центральним інструментом управління цим правовим ризиком є спеціальне договірне кіберзастереження (cyber force majeure clause) – нормативна конструкція, що конкретизує умови, за яких кіберінцидент звільняє сторону від відповідальності або змінює умови виконання договору. Оптимально сконструйоване кіберзастереження має вирішувати п'ять ключових питань:

1. визначення кіберінцидентів, що охоплюються застереженням, – через таксономію видів атак із прямим посиланням на галузеві класифікатори;

2. встановлення стандарту кіберзахисту, дотримання якого є умовою застосування застереження;

3. процедура повідомлення контрагента про настання інциденту і строки такого повідомлення;

4. правові наслідки кіберінциденту – повне звільнення, часткове звільнення, призупинення виконання або зміна умов договору;

5. розподіл ризиків між сторонами у разі, коли кіберінцидент стосується субпідрядника або постачальника хмарних послуг, а не безпосередньо сторони договору.

Відсутність чіткого кіберзастереження у IT-договорі є не нейтральним упущенням, а принциповим вибором на користь невизначеності, що у разі виникнення спору перекладає вирішення всіх цих питань на суд, який, як правило, не має ані спеціальних технічних знань, ані усталеного правового стандарту для їх вирішення.

Особливою і вкрай практично гострою різновидністю проблеми є так звані ланцюгові кіберінциденти – ситуації, коли виконавець IT-договору не зазнає безпосередньої кібератаки, але виявляється нездатним виконати зобов'язання внаслідок компрометації його підрядника, постачальника хмарних послуг або розробника програмного компонента. Атака на SolarWinds (2020), що скомпрометувала тисячі організацій через оновлення ПЗ, яке вони отримали від надійного постачальника, є найбільш показовим прикладом: жертви атаки не мали жодної можливості запобігти їй у власних системах, але зазнали повного порушення функціональності критичних сервісів [6].

З позиції договірного права виникає принципова колізія: виконавець IT-договору, що не виконав зобов'язання через компрометацію свого постачальника, посилається на форс-мажор – але замовник справедливо вказує, що вибір і моніторинг субпідрядників є прямим обов'язком виконавця. Ця колізія відображає ширшу доктринальну проблему – питання про те, чи поширюється форс-мажорний захист на обставини, що знаходяться у «сфері ризику» боржника навіть без його прямої вини. УНІДРУА, Принципи PECL і DCFR у цьому питанні солідарні: форс-мажор не охоплює обставини, що знаходяться у контролі боржника або його

субпідрядників – і ланцюгові кіберінциденти через ненадійного постачальника є саме такими.

Кіберінциденти як обставини непереборної сили в ІТ-договорах є тією сферою, де відсутність системної правової доктрини є не академічною проблемою, а джерелом реальних і масштабних правових конфліктів у найближчі роки – особливо в умовах триваючого збройного конфлікту, що перетворює Україну на один із найбільш кіберактивних середовищ у світі.

Отже, як висновок можна зазначити, що кваліфікація кіберінциденту як форс-мажорної обставини не може ґрунтуватися виключно на факті його настання. Вирішальне значення має оцінка поведінки сторони-боржника, зокрема того, чи були нею вжиті всі розумно необхідні технічні та організаційні заходи для запобігання інциденту або мінімізації його наслідків. Саме тому критерій належної обачності набуває у сфері цифрових відносин спеціалізованого змісту та повинен визначатися з урахуванням сучасних вимог кібербезпеки, галузевих стандартів і кращих практик управління інформаційними ризиками.

ЛІТЕРАТУРА:

1. Чернящук Н., Клещевник К. Аналіз кібератак останніх років: уроки для захисту. *Міжнародна науково-практична конференція «Проблеми комп'ютерних наук, програмного моделювання та безпеки цифрових систем».* 2025, С. 116–118.

2. Маріц Д.О., Пазюк М.В., Уваров І.А. Проблеми доведення форс-мажорних обставин у договірних зобов'язаннях під час дії воєнного стану в Україні. *Електронне наукове видання «Аналітично-порівняльне правознавство».* Випуск № 03, 2025, частина 1. С. 272-278.

3. Юридичні договори у сфері кібербезпеки: як захистити дані та конфіденційність. URL: https://www.bca.education/dogovory-kiberbezpeky/

4. Merck & C., Inc., et al. vs. Ace American Insurance Company, et al. 2023. URL: https://law.justia.com/cases/new-jersey/appellate-division-published/2023/a-1879-21.html

5. Sunburst (кібератака). Вікіпедія – вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Sunburst_(кібератака)