https://doi.org/10.26565/2075-1834-2026-41-32
УДК 341УДК 342.9511:004.056.5:351.861:355.451:338.242

СВИРИДЮК Н.П.
доктор юридичних наук, професор
E-mail: S_N_P_@ukr.net ORCID: https://orcid.org/0000-0001-9772-1119
Одеський державний університет внутрішніх справ
м. Одеса, 65014, вул. Успенська,1

ЦЮПРИК Н.О.
кандидат юридичних наук
E-mail: Tsiyprik@ukr.net ORCID: https://orcid.org/0009-0005-5542-1026
Національна академія внутрішніх справ
м. Київ, 03035, пл. Солом'янська, 1

МІЖНАРОДНІ СТАНДАРТИ ТА ЗАРУБІЖНИЙ ДОСВІД ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

АНОТАЦІЯ. *Вступ.* У статті досліджено міжнародні стандарти та зарубіжний досвід правового забезпечення кіберстійкості в умовах зростання глобальних цифрових загроз. Актуальність теми зумовлена трансформацією кіберстійкості з технічної категорії у стратегічний пріоритет національної та міжнародної безпеки, що особливо важливо для України в умовах воєнних викликів і гібридної агресії. Постановка проблеми статті полягає у фрагментарності та відсутності системного науково-правового узагальнення сучасних міжнародних моделей кіберстійкості, що ускладнює формування цілісної концепції її імплементації в національну політику безпеки України в умовах зростання гібридних та кіберзагроз. Метою статті є комплексний аналіз підходів провідних міжнародних організацій і держав до формування систем кіберстійкості та визначення можливостей імплементації відповідного досвіду в національне законодавство України. Методологічну основу становлять загальнонаукові та спеціально-юридичні методи, зокрема порівняльно-правовий, системно-структурний та формально-логічний аналіз.

Короткий зміст основних результатів дослідження. У роботі розглянуто концептуальні засади кіберстійкості в діяльності НАТО, зокрема її зв'язок із принципом колективної оборони та розвитком інституційної спроможності реагування на кіберзагрози. Проаналізовано нормативно-правову модель Європейського Союзу, включаючи акти CRA, NIS2 та DORA, які формують інтегровану систему цифрової стійкості. Окрему увагу приділено американській моделі, що базується на стандартах NIST та діяльності CISA, а також британському підходу, який поєднує стратегічне управління з розвитком людського капіталу. Обґрунтовано, що ефективна система кіберстійкості формується на основі поєднання правового регулювання, технічних стандартів і публічно-приватного партнерства. Визначено, що для України пріоритетними напрямами є адаптація європейського законодавства, впровадження міжнародних стандартів та підвищення ролі людського капіталу.

Висновок. Встановлено, що кіберстійкість еволюціонує у напрямі системної властивості соціотехнічних систем, яка поєднує правові, організаційні, економічні та технологічні компоненти. Найбільш ефективною визначено гібридну модель, що поєднує регуляторну жорсткість ЄС, інженерні стандарти США, координаційні механізми НАТО та соціотехнічну гнучкість Великої Британії. Для України ключовими напрямами імплементації визначено гармонізацію з європейськими регуляторними актами, розвиток галузевих центрів обміну інформацією та посилення людського капіталу як базового елементу кіберстійкості.

КЛЮЧОВІ СЛОВА*: кіберстійкість, кібербезпека, критична інфраструктура, NIS2, NIST, CRA.*

Як цитувати: Свиридюк Н.П., Цюприк Н.О. Міжнародні стандарти та зарубіжний досвід правового забезпечення кіберстійкост *Вісник Харківського національного університету імені В. Н. Каразіна, серія «Право».* 2026. Вип. 41. С. 341-352. https://doi.org/10.26565/2075-1834-2026-41-32

In cites: N. P. Svyrydiuk, N. O. Tsiyprik (2026) International standards and foreign experience in the legal framework for cyber resilience *The Journal of V.N. Karazin Kharkiv National University, Series "Law"*, (41), P. 341-352. https://doi.org/10.26565/2075-1834-2026-41-32 (in Ukrainian)

Вступ. Сучасний розвиток цифрових технологій та критичної інфраструктури супроводжується зростанням кіберзагроз, що вимагає формування комплексних правових механізмів забезпечення кіберстійкості. У різних країнах сформовано відмінні правові моделі кіберстійкості, що потребує їх системного порівняння та узагальнення. Відсутність єдиного глобального підходу до регулювання кіберстійкості зумовлює необхідність дослідження міжнародного досвіду з метою виявлення ефективних правових рішень та перспектив їх

імплементації в національні правові системи.

Актуальність дослідження зумовлена стрімким зростанням кіберзагроз для критичної інфраструктури та необхідністю формування ефективних міжнародних правових механізмів забезпечення кіберстійкості. У сучасних умовах кіберстійкість розглядається як здатність систем не лише протидіяти атакам, а й забезпечувати безперервність функціонування та відновлення після інцидентів. Ключову роль у цьому відіграють міжнародні стандарти та регуляторні акти, зокрема Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи для забезпечення високого спільного рівня кібербезпеки в Союзі (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 (далі – Директива ЄС NIS2)) [1], стандарти «Інформаційна безпека, кібербезпека та захист приватності - Системи управління інформаційною безпекою – Вимоги» (Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems - Requirements (далі – ISO/IEC 27001)) [2], «Кібербезпека – Керівні принципи щодо безпеки в Інтернеті» (Cybersecurity – Guidelines for Internet security (далі – ISO/IEC 27032)) [3] та рамки Національного інституту стандартів і технологій США (National Institute of Standards and Technology (далі – NIST)) [4], які визначають базові підходи до управління кіберризиками, інцидент-репортингу та координації суб'єктів кібербезпеки. Водночас у різних юрисдикціях спостерігається фрагментарність підходів до правового регулювання кіберстійкості, що актуалізує необхідність порівняльного аналізу зарубіжного досвіду та визначення напрямів гармонізації міжнародних стандартів.

Стан наукового дослідження проблеми. Проблематика забезпечення кіберстійкості як складової національної та міжнародної безпеки перебуває у центрі уваги сучасної правової науки та міждисциплінарних досліджень. Окремі аспекти правового регулювання кібербезпеки, захисту інформаційних ресурсів та функціонування критичної інфраструктури досліджувалися як вітчизняними, так і зарубіжними науковцями.

Водночас, питання щодо міжнародних стандартів і зарубіжного досвіду правового забезпечення кіберстійкості критичної інфраструктури є одними з найбільш активно досліджуваних у сучасній юридичній та міждисциплінарній науці. Її актуальність зумовлена стрімкою цифровізацією критичних систем, зростанням кібератак і необхідністю формування уніфікованих підходів до регулювання кібербезпеки на міжнародному рівні.

Так, зарубіжна наукова література характеризується високим ступенем деталізації нормативних моделей кіберстійкості та їх порівняльного аналізу. Значний інтерес становить дослідження Супангата А. та Тауфікурокмана Т. (Supangat A., Taufiqurokhman T.) [5], у якому порівнюються ключові правові рамки Директиви ЄС NIS2 про кібербезпеку, Закону США 2022 року «Закон про повідомлення про кіберінциденти в критичній інфраструктурі» (Cyber Incident Reporting for Critical Infrastructure Act of 2022 (далі – CIRCIA) [6], Закону ЄС про кібербезпеку (далі – Cybersecurity Act) [7] та інші моделі. Автори доводять, що ефективність кіберстійкості прямо залежить від інтеграції обов'язкових механізмів повідомлення про інциденти та стандартизованих фреймворків управління ризиками.

Подібні висновки містяться у роботі Дафіеля Г. та Баларабе С. (Dafiel G., Balarabe S.) [8], які аналізують правове регулювання цифрових систем охорони здоров'я. Вони підкреслюють роль Загального регламенту про захист даних (General Data Protection Regulation (далі – GDPR)) [9] та ISO/IEC 27001 у формуванні транскордонної кіберстійкості, а також необхідність уніфікації правових підходів до обробки даних.

Окремий напрям досліджень стосується концептуалізації кіберстійкості як правової категорії. Камара І. (Kamara I.) [10] та Байгрейв Л. (Bygrave L.) [11] аналізують еволюцію поняття «кіберстійкість» у правовому контексті, наголошуючи на переході від моделі «кібербезпеки» до більш комплексної моделі стійкості систем. Це дозволяє враховувати не лише захист, а й здатність систем відновлювати функціонування після атак.

У роботах Ріствея Дж. та ін. (Ristvej J. et al.) [12], Лонго А. та ін. (Longo A. et al.) [13] розробляються моделі кіберфізичної стійкості критичної інфраструктури в контексті імплементації Директиви ЄС NIS2. Автори акцентують увагу на інтеграції технічних, організаційних та правових механізмів, що формують єдину архітектуру кіберстійкості.

Важливим напрямом є також дослідження глобального кіберурядування. Верхелст А. та Вутерс Дж. (Verhelst A. та Wouters J.) [14] підкреслюють наявність прогалин у міжнародному регулюванні, що зумовлює фрагментацію підходів між ЄС, НАТО та іншими акторами. Коссефф Дж. (Kosseff J.) [15] пропонує конце-

пцію спільних міжнародних принципів кіберправа, спрямованих на уніфікацію підходів до регулювання кіберпростору.

У контексті порівняльного права Людвігсен К. (Ludvigsen K.) [16] та Такуро К. (Takuro K.) [17] досліджують моделі ЄС і США, обґрунтовуючи необхідність гнучкого регулювання та посилення ролі регуляторних органів. Аналогічно, Узоугбо Н., Ікегву К. та Адевусі А. (Uzougbo N., Ikegwu C., Adewusi A.) [18] аналізують гармонізацію стандартів у фінансовому секторі, демонструючи зближення регуляторних практик у різних регіонах світу.

Українські дослідження у цій сфері формують важливу теоретико-правову базу для аналізу інтеграції національного законодавства до європейських і глобальних стандартів. Так, у праці Шопіної І., Хомякова Д., Христинченко Н., Жукова С. та Шпенова Д. здійснено компаративний аналіз правового та організаційного забезпечення кібербезпеки у провідних країнах, НАТО та ЄС. Автори підкреслюють значення стандартів ISO/IEC 27032 та інституційної ролі державних органів у формуванні кіберстійкості [19]. Це дослідження заклало основу для розуміння взаємозв'язку між технічними стандартами та правовим регулюванням.

Подальший розвиток української наукової думки представлений роботами Довганя О. та Ткачука Т., які проаналізували правові аспекти захисту критичної інфраструктури в контексті міжнародних стандартів NIST, ISO/IEC 27001 та Директиви ЄС NIS2. Автори наголошують на частковій гармонізації українського законодавства з європейськими вимогами та необхідності системного впровадження ризик-орієнтованого підходу [20].

Важливий внесок зроблено у роботі Головка О., Кравченка О., Погребицького М. та Романюка І., які дослідили напрями вдосконалення правового регулювання захисту інформаційних мереж критичної інфраструктури. Автори обґрунтовують потребу гармонізації з Директивою ЄС NIS2, запровадження сертифікаційних механізмів і посилення юридичної відповідальності за кіберінциденти [21].

Викликають зацікавленість роботи Користіна О. та Демедюка С., які у своїх працях приділили увагу підходам НАТО до забезпечення стійкості системи кібербезпеки, зокрема інституційним механізмам, принципам колективного захисту та практики реагування на кіберзагрози [22], проблемам формування національної системи кіберстійкості України з акцентом на захист критичної інфраструктури та розвиток механізмів реагування на кіберінциденти [23] та розвитку спроможностей державних органів у сфері протидії кіберзлочинності [24].

Таким чином, українська доктрина поступово переходить від описових моделей до практично орієнтованих регуляторних пропозицій.

Зазначене свідчить про те, що дослідження міжнародних стандартів та зарубіжного досвіду правового забезпечення кіберстійкості демонструє їх високий рівень системності, нормативної узгодженості та практичної ефективності, що досягається шляхом інтеграції правових, організаційних і технічних механізмів. У провідних державах кіберстійкість розглядається як ключовий елемент національної та колективної безпеки, зокрема в межах Європейського Союзу та НАТО. Водночас для України ця проблематика має не лише теоретичне, а й стратегічне значення, з огляду на триваючу гібридну агресію та постійний вплив кіберзагроз на критичну інфраструктуру держави. Україна фактично виступає як простір апробації сучасних підходів до кіберстійкості в умовах реальних кіберконфліктів, що формує унікальний практичний досвід, релевантний для міжнародної спільноти. Попри це, національна наукова доктрина поки що характеризується фрагментарністю та недостатнім рівнем системного узагальнення міжнародних стандартів. Це зумовлює необхідність поглиблення наукових досліджень, спрямованих на адаптацію та імплементацію кращих зарубіжних практик, а також формування цілісної концепції правового забезпечення кіберстійкості в Україні як невід'ємної складової європейського та глобального безпекового простору.

Метою статті є комплексний аналіз міжнародних стандартів та зарубіжного досвіду правового забезпечення кіберстійкості, а також визначення можливостей їх імплементації в національну правову систему України з урахуванням сучасних безпекових викликів.

Для досягнення поставленої мети передбачається вирішення таких завдань: дослідити концептуальні підходи до розуміння кіберстійкості в діяльності міжнародних організацій; проаналізувати нормативно-правові моделі Європейського Союзу, США та Великобританії; а також визначити перспективні напрями вдосконалення національного законодавства України у цій сфері.

Основні результати дослідження. На сучасному етапі еволюції міжнародних відносин кіберстійкість вийшла за межі вузько технічного поняття та набула статусу одного з визначальних компонентів глобальної системи

безпеки. В умовах зростаючої цифрової взаємозалежності та високого рівня інтегрованості національних інфраструктур навіть обмежені за масштабом кіберінциденти здатні провокувати ланцюгові наслідки, що поширюються на економічну стабільність і політичний баланс на міжнародному рівні. У зв'язку з цим дедалі більшого значення набуває концепція колективної кіберстійкості, яка передбачає спільну відповідальність держав, приватного сектору та міжнародних інституцій за протидію кіберзагрозам, а також координацію їхніх дій у межах інтегрованих механізмів запобігання та реагування.

У розвиток зазначених положень слід підкреслити, що провідне місце у формуванні нормативно-концептуальних засад кіберстійкості належить НАТО. Так, забезпечення стійкості, згідно зі статтею 3 Північноатлантичного договору, розглядається як фундаментальний компонент системи колективної оборони. Важливо, що сучасне трактування цього поняття закріплено 2016 року на Варшавському саміті у «Зобов'язанні щодо посилення стійкості», де кіберпростір визначено як окремий операційний домен. Водночас, у межах підходів Альянсу стійкість інтерпретується не лише як технічна надійність інформаційних систем, а як комплексна спроможність держави гарантувати безперервне функціонування критично важливих інституцій та послуг у кризових умовах. Значний внесок у розвиток практичних механізмів забезпечення кіберстійкості здійснює Кооперативний центр передового досвіду з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence (далі – CCDCOE)) [25], який розробляє методологічні підходи та організовує спеціалізовані навчання, зокрема міжнародні кібернавчання з кібероборони «Locked Shields», спрямовані на відпрацювання сценаріїв відновлення інфраструктури після кібератак [26, с. 99].

Логічним продовженням цього підходу є системність політики НАТО у сфері кіберстійкості, що проявляється у комплексному залученні всіх релевантних суб'єктів безпеки та послідовному розвитку інституційної спроможності до реагування на сучасні загрози [27, с. 129]. Важливо відзначити, що еволюція концепції стійкості відображає загальні трансформації безпекового середовища: від вузького розуміння як здатності протидіяти переважно військовим загрозам до багатовимірної політики, що інтегрує цивільний, економічний, інформаційний та технологічний виміри. Отже, якщо раніше стійкість розглядалася як похідна від колективної оборони, то сьогодні вона функціонує як відносно автономний напрям діяльності Альянсу, що має власні інструменти реалізації та стратегічні пріоритети.

З огляду на зазначену еволюцію, суттєві зміни безпекового середовища після 2014 року стали каталізатором інституційного закріплення політики стійкості в межах НАТО. Зокрема, було ухвалено «План дій щодо забезпечення готовності» [28], який передбачав зміцнення оборонних спроможностей, підвищення оперативної мобільності, вдосконалення координаційних механізмів та розвиток систем кризового управління. Подальша конкретизація цих підходів відбулася у 2016 році через прийняття Керівних принципів, які визначили ключові функціональні напрями забезпечення стійкості, серед яких: безперервність діяльності уряду, енергетична безпека, управління міграційними процесами, стабільність у сфері продовольства та водопостачання, готовність до масових втрат, а також стійкість транспортної і комунікаційної інфраструктури [29; 30]. Таким чином, стійкість була інституціоналізована як комплексна міжсекторальна політика.

Водночас реалізація зазначених принципів супроводжувалася активним розвитком практичних інструментів у кіберсфері. Зокрема, йдеться про створення спеціалізованих команд реагування на кіберінциденти, укладення угод щодо захищеного обміну інформацією, посилення ролі CCDCOE, а також розширення співпраці з інноваційними технологічними компаніями. Важливим аспектом є також імплементація національних стратегій кібербезпеки держав-членів, що забезпечує узгодженість політик та сприяє підвищенню рівня колективної стійкості [30]. У ширшому контексті протидії гібридним загрозам НАТО акцентує увагу на інтеграції кіберзахисту в оборонні операції, розвитку національних спроможностей, обміні розвідувальними даними та поглибленні взаємодії з міжнародними партнерами, зокрема інституціями Європейського Союзу [29].

Логічним продовженням зазначених процесів є посилення ролі публічно-приватного партнерства у сфері забезпечення кіберстійкості. Така тенденція обумовлена тим, що значна частина критичної інфраструктури перебуває у приватній власності, що об'єктивно обмежує можливості держави діяти автономно. У відповідь на це формується модель так званих «коаліцій стійкості», в межах яких державні інституції виконують передусім координаційну та фасилітативну функцію. Вони забезпечують організацію обміну інформацією, розробку спільних протоколів реагу-

вання та впровадження інструментів оцінювання ризиків, таких як, наприклад, методика оцінки кіберстійкості (Cyber Resilience Review (далі – CRR)) [31, с. 303]. У результаті відбувається становлення багаторівневої системи кіберстійкості, що поєднує нормативно-правові механізми, технічні стандарти, політичні зобов'язання та економічні стимули, забезпечуючи комплексний підхід до управління кіберризиками.

У контексті загальноєвропейських трансформацій безпекової політики особливої уваги заслуговує підхід Європейського Союзу, який здійснив комплексну модернізацію нормативно-правової бази, перейшовши до моделі інтегрованої цифрової стійкості. Така трансформація відображає усвідомлення необхідності системного регулювання кіберризиків на всіх етапах функціонування цифрового середовища. В основі цієї моделі лежить проактивний підхід до управління життєвим циклом цифрових продуктів і послуг, що передбачає запобігання виникненню вразливостей ще на етапі їхнього проєктування та впровадження. Концептуально ця модель поєднує три взаємопов'язані компоненти: горизонтальне регулювання, секторну безпеку та забезпечення фінансової стабільності, що у сукупності формують цілісну архітектуру цифрової стійкості.

Ключовим інструментом регуляторної політики ЄС став Акт Європейського Союзу про кіберстійкість (Cyber Resilience Act (далі – CRA)) [32], який встановлює обов'язкові вимоги до безпеки продуктів із цифровими елементами. Його принципова новизна полягає у зміщенні акценту з реагування на інциденти до превентивного забезпечення безпеки. Зокрема, документ імплементує принципи «security by design (безпека на етапі проєктування)» та «security by default (безпека за замовчуванням)», відповідно до яких вимоги кібербезпеки інтегруються безпосередньо у процес розробки продуктів. Водночас суттєво змінюється розподіл відповідальності: вона покладається передусім на виробників і постачальників, а не на кінцевих користувачів. У результаті формується нова модель функціонування внутрішнього ринку ЄС, у межах якої кіберстійкість виступає обов'язковою передумовою доступу до нього, що стимулює підвищення загального рівня безпеки цифрової продукції [33; 34; 35].

Логічним доповненням CRA є Директива ЄС NIS2 [1], яка значно розширює сферу регуляторного впливу та поглиблює вимоги до суб'єктів критичної інфраструктури. Зокрема, вона запроваджує більш жорсткі стандарти управління кіберризиками, підзвітності та реагування на інциденти. Особливу увагу в документі приділено концепції «стійкості ланцюгів постачання», яка передбачає поширення вимог кібербезпеки не лише на безпосередніх операторів, але й на їхніх партнерів і постачальників. Такий підхід відображає мережеву природу сучасних загроз і сприяє формуванню розгалуженої системи безпеки, що є критично важливою для функціонування таких секторів, як енергетика, транспорт і охорона здоров'я [36]. Таким чином, Директива ЄС NIS2 посилює інтеграційний характер політики кіберстійкості ЄС.

У свою чергу, у фінансовому секторі ключову роль відіграє регламент Акту Європейського Союзу про цифрову операційну стійкість (Digital Operational Resilience Act (далі – DORA) [37], який конкретизує вимоги до забезпечення операційної стійкості фінансових установ. Він встановлює комплексні стандарти управління ризиками, включаючи обов'язкове тестування систем, контроль за постачальниками ІКТ-послуг та розробку механізмів відновлення після кібератак. Важливо підкреслити, що DORA інституціоналізує підхід, відповідно до якого фінансова стабільність безпосередньо залежить від рівня кіберстійкості, тим самим інтегруючи питання кібербезпеки у ширший контекст економічної безпеки [38].

Завершальним елементом цієї системи виступає інституційне забезпечення політики кіберстійкості ЄС. Зокрема, діяльність Агентства Європейського Союзу з кібербезпеки (European Union Agency for Cybersecurity (далі – ENISA)) [39] та мережі національних команд реагування на комп'ютерні інциденти (Computer Security Incident Response Teams (далі – CSIRTs) [40] спрямована на координацію реагування, розвиток спільних стандартів та впровадження механізмів сертифікації. Водночас стратегічні документи ЄС передбачають створення так званого «Cyber Shield» [41] – національних та міжнародних кібернавчань з кіберзахисту. Це мережі центрів моніторингу кіберзагроз із використанням технологій штучного інтелекту, що має на меті підвищення спроможності до раннього виявлення та запобігання атакам. У підсумку, модель Європейського Союзу базується на принципах солідарності, відповідальності та прозорості, поєднуючи нормативно-правові, інституційні та технологічні інструменти. Саме ця комплексність і системність робить її важливим орієнтиром для України в контексті євроінтеграційних процесів та адаптації національної політики кібербезпеки.

У продовження аналізу регуляторної моделі Європейського Союзу доцільно звернутися до досвіду Сполучених Штатів Америки, який демонструє альтернативний, більш гнучкий і технологічно орієнтований підхід до забезпечення кіберстійкості. Якщо європейська модель ґрунтується переважно на нормативній імперативності та уніфікації правил, то американська практика характеризується поєднанням державного регулювання, стандартизації та ринкових механізмів, що забезпечує високу адаптивність до динамічних кіберзагроз. Такий підхід відображає прагнення до балансу між безпекою та інноваційним розвитком.

Центральним елементом інституційної архітектури кіберстійкості США виступає Агентство кібербезпеки та захисту інфраструктури (Cybersecurity and Infrastructure Security Agency (далі – CISA)) [42], яке координує взаємодію між державними органами та приватним сектором.

Подальша інституціоналізація цих підходів відбулася через ухвалення Виконавчого указу Президента США №14028 «Про вдосконалення кібербезпеки національної кіберінфраструктури» (Executive Order 14028 Improving the Nation's Cybersecurity) [43], який визначив сучасні стандарти кібербезпеки для федеральних інформаційних систем. Зокрема, документ передбачає обов'язкове впровадження багатофакторної автентифікації, широке застосування криптографічного захисту та модернізацію застарілої інфраструктури. Водночас принциповим є закріплення моделі спільної відповідальності держави та приватного сектору, що відображає реальну структуру володіння критичною інфраструктурою та підкреслює необхідність координації зусиль у сфері кіберзахисту. Таким чином, кіберстійкість у США розглядається як результат синергії публічних і приватних акторів.

Методологічну основу цієї моделі становлять стандарти NIST [4], які формалізують ключові принципи забезпечення стійкості, зокрема адаптивність, надлишковість і сегментацію мереж. Їхня особливість полягає у гнучкості застосування, що дозволяє адаптувати загальні рекомендації до специфіки різних секторів економіки.

У результаті формуються системи, здатні підтримувати виконання критично важливих функцій навіть у разі часткового ураження, реалізуючи концепцію так званої «граціозної деградації» [44, с. 113–114]. Такий підхід істотно розширює традиційне розуміння кіберзахисту, акцентуючи увагу на безперервності функціонування.

Характерною рисою американської моделі є також визначальна роль приватного сектору, передусім великих технологічних компаній, які забезпечують функціонування значної частини цифрової інфраструктури. У цьому контексті особливого значення набувають хмарні технології, що розглядаються як ефективний інструмент підвищення відмовостійкості, масштабованості та швидкості відновлення інформаційних систем. Саме інтеграція інноваційних рішень із державними стратегіями формує динамічну та адаптивну модель кіберстійкості, здатну ефективно реагувати на сучасні виклики.

Таким чином, на відміну від нормативно-орієнтованої моделі Європейського Союзу, підхід США демонструє переваги гнучкого регулювання та технологічної інноваційності. У сукупності ці моделі формують взаємодоповнювальні парадигми забезпечення кіберстійкості, що створює широке поле для їх адаптації в національних умовах, зокрема в Україні, яка прагне інтегрувати як регуляторні стандарти ЄС, так і практичні інструменти та технологічні підходи США.

У продовження розгляду національних моделей кіберстійкості доцільно звернутися до досвіду Великої Британії, який демонструє послідовну еволюцію у напрямі формування інтегрованої державної кіберпотужності. У цій моделі кіберстійкість розглядається не як ізольований технічний компонент, а як невід'ємна складова ширшої концепції національної безпеки та стратегічної спроможності держави в цифрову епоху. Відповідно, національна стратегія орієнтована на проактивне формування безпечного цифрового середовища, що базується на розподілі відповідальності між державними інституціями, приватним сектором та громадянським суспільством. Центральним елементом цієї архітектури виступає Національний центр кібербезпеки (National Cyber Security Centre (далі – NCSC)) [45], який виконує координуючу, аналітичну та операційну функції у сфері реагування на кіберзагрози [31; 32]. Така інституційна модель забезпечує поєднання стратегічного управління з високим рівнем оперативної гнучкості.

Подальшого розвитку ця система набуває на рівні регіональних ініціатив, серед яких особливої уваги заслуговує шотландський підхід. Його специфіка полягає у значній орієнтації на розвиток людського капіталу, підвищення рівня цифрової грамотності населення та підтримку малого і середнього бізнесу як ключових елементів кіберстійкості. У цьому контексті кібербезпека інтегрується у ширшу кон-

цепцію суспільного добробуту, що дозволяє розглядати її не лише як елемент державної політики безпеки, але й як складову соціально-економічного розвитку. Важливою особливістю даного підходу є реалізація принципу «знизу вгору», за якого ініціативи формуються на рівні місцевих спільнот і поступово інтегруються у національну систему кіберзахисту [46].

Синергія загальнонаціональної британської моделі та регіональних практик забезпечує формування багаторівневої системи кіберстійкості, у якій поєднуються стратегічне централізоване управління та локальна адаптивність. Така структура дозволяє ефективно враховувати специфіку різних регіонів і секторів економіки, одночасно зберігаючи єдині стандарти реагування на кіберзагрози. Додатково важливим елементом цієї моделі є поступова інтеграція кібер- та фізичної безпеки, що відображає сучасні тенденції конвергенції загроз у цифровому та матеріальному просторах. Паралельно відбувається розвиток автоматизованих систем захисту та сервісів кібербезпеки, які підвищують швидкість реагування та знижують людський фактор ризику.

У результаті формується концепція так званого «колективного імунітету» держави, відповідно до якої стійкість забезпечується не лише через інституційні механізми, але й через загальний рівень цифрової зрілості суспільства, бізнесу та державних структур [47, с. 96]. Такий підхід дозволяє розглядати кіберстійкість як комплексну властивість соціотехнічної системи, що формується на перетині технологічних, управлінських та суспільних факторів.

З урахуванням наведеного, міжнародний та зарубіжний досвід набуває особливої актуальності для України. Це зумовлено тим, що в умовах тривалого впливу гібридних загроз стійкість виступає базовою характеристикою сектору безпеки і оборони. У цьому контексті вона розглядається як інтегрована властивість системи, що передбачає здатність до безперервного функціонування, адаптації до змін зовнішнього середовища, протидії дестабілізуючим чинникам та швидкого відновлення після криз із збереженням керованості та інституційної цілісності [48, с. 23–24]. Таким чином, йдеться про перехід від реактивної до проактивної моделі забезпечення безпеки.

Формування нормативно-правової бази стійкості в Україні має відносно недавній, але динамічний характер. Якщо у Стратегії національної безпеки 2015 року поняття стійкості використовувалося обмежено і не було системоутворюючим [22; 29; 49], то вже у Стратегії 2020 року воно визначене як один із ключових принципів державної політики поряд із стримуванням і взаємодією [22; 50]. Зазначений документ закладає основи формування цілісної національної системи стійкості, що включає оцінювання ризиків, стратегічне планування, міжвідомчу координацію, розвиток професійних компетенцій та ефективну комунікацію з населенням як важливий елемент суспільної стійкості [22]. Відтак, можна констатувати поступовий перехід до інституціоналізації стійкості як базового принципу державної політики у сфері національної безпеки.

Подальший розвиток окреслені підходи отримали у Стратегії кібербезпеки України 2021 року, яка концептуалізує стійкість до кіберзагроз як один із визначальних індикаторів ефективності державної політики у сфері національної безпеки. На відміну від попередніх документів, у цій стратегії акцент зміщується з реагування на інциденти до формування проактивної системи запобігання загрозам. Зокрема, йдеться про підвищення інституційної спроможності держави, зміцнення ролі приватного сектору та формування культури кібербезпеки серед громадян. Окрему увагу приділено розвитку кадрового потенціалу, стимулюванню інновацій та становленню конкурентоспроможного ринку послуг у сфері кібербезпеки, що у сукупності створює передумови для довгострокової стійкості національної кіберекосистеми [22; 51]. Таким чином, стійкість поступово інтегрується у всі рівні державної політики як наскрізний принцип.

Висновки. У результаті проведеного аналізу сучасних підходів до формування кіберстійкості у міжнародній практиці дозволяє констатувати її системну трансформацію з техніко-операційної категорії у комплексний міждисциплінарний феномен, що інтегрує безпекові, правові, економічні та соціотехнічні виміри. У сучасних умовах кіберстійкість виступає не лише інструментом протидії кіберзагрозам, але й фундаментальним елементом забезпечення стабільності держав, функціонування критичної інфраструктури та глобальної економічної взаємозалежності.

Порівняльний аналіз моделей НАТО, Європейського Союзу, США та Великої Британії засвідчив, що формування кіберстійкості відбувається за різними інституційними логіками, однак зберігає спільну тенденцію до інтеграції трьох ключових компонентів: стратегічного управління ризиками, нормативно-правової інституціоналізації та технологічної адаптивності. Модель НАТО акцентує увагу на колективній обороні та інституційній коорди-

нації; Європейський Союз – на регуляторній уніфікації та юридичній імперативності; США – на поєднанні державного управління з ринковими механізмами та технологічними інноваціями; Велика Британія – на соціотехнічній інтеграції та багаторівневій взаємодії центр-регіони. Узагальнення міжнародного досвіду дозволяє стверджувати, що найбільш ефективною є гібридна модель кіберстійкості, яка поєднує нормативну жорсткість регуляторних підходів ЄС (CRA, Директива ЄС NIS2), інженерну стандартизацію США (NIST), стратегічну координацію НАТО та соціотехнічну адаптивність Великої Британії. Така інтеграція забезпечує формування багаторівневої системи захисту, здатної функціонувати в умовах динамічних та асиметричних кіберзагроз.

Для України результати дослідження мають прикладне значення в контексті формування національної системи кіберстійкості. Її подальший розвиток має ґрунтуватися на імплементації європейських регуляторних стандартів, адаптації американських технічних підходів, використанні інституційних практик НАТО та розвитку соціальної складової кібербезпеки. Особливого значення набуває запровадження обов'язкової сертифікації цифрових продуктів та розвиток галузевих центрів обміну інформацією та посилення людського капіталу як ключового чинника кіберстійкості.

У підсумку, кіберстійкість доцільно розглядати як інтегральну властивість складних соціотехнічних систем, що визначає їх здатність не лише протидіяти кіберзагрозам, але й зберігати функціональну безперервність, адаптивність та здатність до відновлення в умовах невизначеності. Перспективи подальших досліджень пов'язані з поглибленим аналізом механізмів інтеграції штучного інтелекту в системи кіберзахисту та формуванням моделей проактивного управління кіберризиками на національному та міжнародному рівнях..

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

2. ISO/IEC 27001 Information Security Management Systems. ISO. URL: https://www.iso.org/isoiec-27001-information-security.html

3. ISO/IEC 27032:2023 Cybersecurity – Guidelines for Internet security. URL: https://www.iso.org/standard/76070.html

4. National Institute of Standards and Technology (NIST). URL: https://www.nist.gov

5. Supangat, A., & Taufiqurokhman, T. (2025). Legal Design and Cyber Resilience: A Comparative Study of Cybersecurity Frameworks for Critical Infrastructure in Five Jurisdictions. Legalis: Journal of Law Review. DOI: https://doi.org/10.61978/legalis.v3i4.1121

6. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). URL: https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

7. The EU Cybersecurity Act. URL: https://eur-lex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html

8. Dafiel, G., & Balarabe, S. (2025). Engineering Law and Cybersecurity in Digital Health: Legal-Informatics Frameworks for Regulating Cross-Border Data Interoperability, Liability, and Resilience in Public Health Communication Systems. International Journal of Research and Scientific Innovation. DOI: https://doi.org/10.51244/ijrsi.2025.1215000139p

9. General Data Protection Regulation.URL: https://gdpr-info.eu/

10. Kamara, I. (2024). European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience. Innovation: The European Journal of Social Science Research. Vol. 37. P. 1441 - 1460. DOI: https://doi.org/10.1080/13511610.2024.2349626

11. Bygrave, L. (2022). Cyber Resilience versus Cybersecurity as Legal Aspiration. 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon). Vol. 700. P. 27-43. DOI: https://doi.org/10.23919/cycon55549.2022.9811084)

12. Ristvej, J., Tonhauser, M., Chovanec, D., Kubás, J., Kollár, B., & Zamiar, Z. (2025). Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. Scientific Reports. Vol. 15. DOI: https://doi.org/10.1038/s41598-025-12829-3

13. Longo, A., Ardebili, A., Lazari, A., & Ficarella, A. (2025). Cyber–Physical Resilience: Evolution of Concept, Indicators, and Legal Frameworks. Electronics. DOI: https://doi.org/10.3390/electronics14081684

14. Verhelst, A., & Wouters, J. (2020). Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. International Organisations Research Journal. DOI: https://doi.org/10.17323/1996-7845-2020-02-07

15. Kosseff, J. (2018). Developing collaborative and cohesive cybersecurity legal principles. 2018 10th International Conference on Cyber Conflict (CyCon). P. 283-298. DOI: https://doi.org/10.23919/cycon.2018.8405022

16. Ludvigsen, K. (2025). Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law. ArXiv, abs/2503.07250. DOI: https://doi.org/10.48550/arxiv.2503.07250

17. Takuro, K. (2023). Exploring cybersecurity law evolution in safeguarding critical infrastructure against ransomware, state-sponsored attacks, and emerging quantum threats. International Journal of Science and Research Archive. DOI: https://doi.org/10.30574/ijsra.2023.10.2.1019

18. Uzougbo, N., Ikegwu, C., & Adewusi, A. (2024). Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. International Journal of Science and Research Archive. DOI: https://doi.org/10.30574/ijsra.2024.12.1.0802

19. Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). Cybersecurity: legal and organizational support in leading countries, nato and eu standards. Journal of Security and Sustainability Issues. Vol. 9. P. 977-992. DOI: https://doi.org/10.9770/jssi.2020.9.3(22)

20. Dovhan, O., & Tkachuk, T. (2024). Legal aspects of critical infrastructure cybersecurity provision: national and international dimension. Information and Law. DOI: https://doi.org/10.37750/2616-6798.2024.4(51).317970

21. Holovko, O., Kravchenko, O., Pogrebytskyi, M., & Romaniuk, I. (2025). Ways to improve legal regulation of critical infrastructure information networks protection. Social and Legal Studios. DOI: https://doi.org/10.32518/sals1.2025.70

22. Демедюк С.В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. Наука і правоохорона. 2023. № 1(59). С.77-85. DOI: https://doi.org/10.36486/np.2023.1(59).8ь

23. Демедюк С.В. Розбудова національної кіберстійкості та захист критично важливої інформаційної інфраструктури. Наука і правоохорона. 2023. № 2(60). С.78-85. DOI: https://doi.org/10.36486/np.2023.2(60).8

24. Демедюк С.В. Реалізація спроможності суб'єктів системи протидії кіберзлочинності. Наука і правоохорона. 2024. № 1(63). С.133-141. DOI: https://doi.org/10.36486/np.2024.1(63).13

25. Cooperative Cyber Defence Centre of Excellence (CCDCOE). NATO. URL: https://ccdcoe.org

26. Tiirmaa-Klaar H. (2016). Building national cyber resilience and protecting critical information infrastructure. Journal of Cyber Policy. Vol. 1, No. 1. P. 94–106.

27. Федієнко О.П. Міжнародні стандарти оцінки кіберстійкості. Інформація і право. 2024. № 3(50) С. 124-135. DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311680

28.NATO's Readiness Action Plan. Strategic Benefits and Outstanding Challenges. URL: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-10_Issue-1/Arnold.pdf

29.Веселова Л.Ю. Кібернетична безпека в умовах гібридної війни: адміністративно-правові засади: монографія. Одеса: Видавничий дім «Гельветика». 2020. 488 с.

30. NATO Defence Ministers agree to enhance collective defence and deterrence. URL: https://www.nato.int/cps/en/natohq/news_132356.htm?selectedLocale=en

31.Herrington L., Aldrich R. (2013).The Future of Cyber-Resilience in an Age of Global Complexity. Politics. Vol. 33(4). P. 299–310.

32. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

33.EU Cyber Resilience Act: Briefing. European Parliamentary Research Service. 2024. 12 p. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf

34. The Cyber Resilience Act: Summary of the legislative text. An official website of the European Union.URL: https://digital-strategy.ec.europa.eu/en/policies/cra-summary

35. Overview EU Cyber Resilience Act. ABB. 2024. 5 p. URL: https://library.e.abb.com/public/c87c6a5acc7443e19a6ed0e4c72d314b/9AKK108471A6145_en_A_Cybersecurity%20Guide%20EU%20CRA.pdf?x-sign=ItWWeq6GekkG8yFqPKIx87Bt%2BNxMtBWxIZYsabwKnmJgnQEwM8sYWMEd6ZJt21Lv

36. The NIS2 Directive: A high common level of cybersecurity in the EU. 2023. 13 p. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

37. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

38. European Union Cyber Resilience Act: A Compliance Guide for Connected Devices. DigiCert. 2025. 8 p. URL: https://www.digicert.com/content/dam/digicert/pdfs/whitepaper/digicert-eu-cra-whitepaper-en.pdf

39. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu

40. Computer Security Incident Response Team (CSIRT). URL: https://www.csirt.org/

41. Cyber Shield .URL: https://www.cybershield.krd/home

42.Cybersecurity and Infrastructure Security Agency (CISA). Official Website. URL: https://www.cisa.gov

43. Executive Order 14028 on Improving the Nation's Cybersecurity. The White House, 2021. URL: https://www.govinfo.gov/content/pkg/DCPD-202100401/pdf/DCPD-202100401.pdf

44. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST / Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Special Publication 800-160, Vol. 2. 2021. 294 p. DOI: https://doi.org/10.6028/NIST.SP.800-160v2r1

45. National Cyber Security Centre. URL: https://www.ncsc.gov.uk

46. The Strategic Framework for a Cyber Resilient Scotland. Scottish Government. 2021. 39 p. URL: https://dera.ioe.ac.uk/id/eprint/37463/1/strategic-framework-cyber-resilient-scotland%20%28redacted%29.pdf

47. Wilding N. (2016). Cyber resilience: How important is your reputation? How effective are your people? Business Information Review. Vol. 33, No. 2. P. 94–99.

48. Резнікова О.О. Забезпечення стійкості держави і суспільства до терористичної загрози в Україні та світі. Стратегічні пріоритети. 2017. № 3 (44). С. 22-28.

49. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 р. №287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015

50. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 р. №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

51. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

Внесок авторів: всі автори зробили рівний внесок у цю роботу
Конфлікт інтересів: автори повідомляють про відсутність конфлікту інтересів

Стаття надійшла до редакції 02.03.2026 Переглянуто 06.04.2026.
Стаття рекомендована до друку 20.05.2026 Опубліковано 30.05.2026

N.P. SVYRYDIUK
DSc (Law), Professor
E-mail: S_N_P_@ukr.net ORCID: https://orcid.org/0000-0001-9772-1119
Odessa State University of Internal Affairs
Odessa, 65014, 1 Uspenska Street

N.O. TSIYPRIK
PhD in Law
E-mail: Tsiyprik@ukr.net ORCID: https://orcid.org/0009-0005-5542-1026
National Academy of Internal Affairs
Kyiv, 03035, 1 Solomyanska Square

INTERNATIONAL STANDARDS AND FOREIGN EXPERIENCE IN THE LEGAL FRAMEWORK FOR CYBER RESILIENCE

ANNOTATION. *Introduction.* This article examines international standards and foreign experience in the legal framework for cyber resilience amid growing global digital threats. The relevance of the topic stems from the transformation of cyber resilience from a technical category into a strategic priority for national and international security, which is particularly important for Ukraine in the context of military challenges and hybrid aggression. The problem addressed in the article lies in the fragmentary nature and lack of a systematic scientific and legal synthesis of contemporary international models of cyber resilience, which complicates the formation of a coherent concept for its implementation into Ukraine's national security policy in the context of growing hybrid and cyber threats. The aim of the article is to provide a comprehensive analysis of the approaches of leading international organisations and states to the development of cyber resilience systems and to identify opportunities for implementing relevant experience into Ukraine's national legislation. The methodological framework comprises general scientific and specialised legal methods, in particular comparative legal, systemic-structural and formal-logical analysis.

Summary of the main findings of the study. This paper examines the conceptual foundations of cyber resilience within NATO's activities, in particular its link to the principle of collective defence and the development of institutional capacity to respond to cyber threats. The regulatory framework of the European Union is analysed, including the CRA, NIS2 and DORA regulations, which form an integrated digital resilience system. Particular attention is paid to the American model, based on NIST standards and CISA, as well as the British approach, which combines strategic management with human capital development. It is argued that an effective cyber resilience system is formed on the basis of a combination of legal regulation, technical standards and public-private partnerships. It is determined that the priority areas for Ukraine are the adaptation of European legislation, the implementation of international standards and the enhancement of the role of human capital.

Conclusion. It has been established that cyber resilience is evolving into a systemic property of socio-technical systems, combining legal, organisational, economic and technological components. The hybrid model, combining the regulatory rigour of the EU, the engineering standards of the US, the coordination mechanisms of NATO and the socio-technical flexibility of the UK, has been identified as the most effective. For Ukraine, the key areas for implementation are identified as harmonisation with European regulatory acts, the development of sectoral information exchange centres, and the strengthening of human capital as a fundamental element of cyber resilience.

KEY WORDS: *cyber resilience, cybersecurity, critical infrastructure, NIS2, NIST, CRA.*

REFERENCES

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
2. ISO/IEC 27001 Information Security Management Systems. ISO. URL: https://www.iso.org/isoiec-27001-information-security.html
3. ISO/IEC 27032:2023 Cybersecurity – Guidelines for Internet security. URL: https://www.iso.org/standard/76070.html
4. National Institute of Standards and Technology (NIST). URL: https://www.nist.gov
5. Supangat, A., & Taufiqurokhman, T. (2025). Legal Design and Cyber Resilience: A Comparative Study of Cybersecurity Frameworks for Critical Infrastructure in Five Jurisdictions. Legalis: Journal of Law Review. DOI: https://doi.org/10.61978/legalis.v3i4.1121
6. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). URL: https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements
7. The EU Cybersecurity Act. URL: https://eur-lex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html
8. Dafiel, G., & Balarabe, S. (2025). Engineering Law and Cybersecurity in Digital Health: Legal-Informatics Frameworks for Regulating Cross-Border Data Interoperability, Liability, and Resilience in Public Health Communication Systems. International Journal of Research and Scientific Innovation. DOI: https://doi.org/10.51244/ijrsi.2025.1215000139p
9. General Data Protection Regulation.URL: https://gdpr-info.eu/

10. Kamara, I. (2024). European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience. Innovation: The European Journal of Social Science Research. Vol. 37. P. 1441 - 1460. DOI: https://doi.org/10.1080/13511610.2024.2349626

11. Bygrave, L. (2022). Cyber Resilience versus Cybersecurity as Legal Aspiration. 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon). Vol. 700. P. 27-43. DOI: https://doi.org/10.23919/cycon55549.2022.9811084)

12. Ristvej, J., Tonhauser, M., Chovanec, D., Kubás, J., Kollár, B., & Zamiar, Z. (2025). Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. Scientific Reports. Vol. 15. DOI: https://doi.org/10.1038/s41598-025-12829-3

13. Longo, A., Ardebili, A., Lazari, A., & Ficarella, A. (2025). Cyber–Physical Resilience: Evolution of Concept, Indicators, and Legal Frameworks. Electronics. DOI: https://doi.org/10.3390/electronics14081684

14. Verhelst, A., & Wouters, J. (2020). Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. International Organisations Research Journal. DOI: https://doi.org/10.17323/1996-7845-2020-02-07

15. Kosseff, J. (2018). Developing collaborative and cohesive cybersecurity legal principles. 2018 10th International Conference on Cyber Conflict (CyCon). P. 283-298. DOI: https://doi.org/10.23919/cycon.2018.8405022

16. Ludvigsen, K. (2025). Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law. ArXiv, abs/2503.07250. DOI: https://doi.org/10.48550/arxiv.2503.07250

17. Takuro, K. (2023). Exploring cybersecurity law evolution in safeguarding critical infrastructure against ransomware, state-sponsored attacks, and emerging quantum threats. International Journal of Science and Research Archive. DOI: https://doi.org/10.30574/ijsra.2023.10.2.1019

18. Uzougbo, N., Ikegwu, C., & Adewusi, A. (2024). Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. International Journal of Science and Research Archive. DOI: https://doi.org/10.30574/ijsra.2024.12.1.0802

19. Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). Cybersecurity: legal and organizational support in leading countries, nato and eu standards. Journal of Security and Sustainability Issues. Vol. 9. P. 977-992. DOI: https://doi.org/10.9770/jssi.2020.9.3(22)

20. Dovhan, O., & Tkachuk, T. (2024). Legal aspects of critical infrastructure cybersecurity provision: national and international dimension. Information and Law. DOI: https://doi.org/10.37750/2616-6798.2024.4(51).317970

21. Holovko, O., Kravchenko, O., Pogrebytskyi, M., & Romaniuk, I. (2025). Ways to improve legal regulation of critical infrastructure information networks protection. Social and Legal Studios. DOI: https://doi.org/10.32518/sals1.2025.70

22. Demediuk S.V., Korystin O.Ie. Stiikist systemy kiberbezpeky ta yii zabezpechennia v NATO. Nauka i pravookhorona. 2023. № 1(59). S.77-85. DOI: https://doi.org/10.36486/np.2023.1(59).8ь (in Ukrainian)

23. Demediuk S.V. Rozbudova natsionalnoi kiberstiikosti ta zakhyst krytychno vazhlyvoi informatsiinoi infrastruktury. Nauka i pravookhorona. 2023. № 2(60). S.78-85. DOI: https: //doi.org/10.36486/np.2023.2(60).8

24. Demediuk S.V. Realizatsiia spromozhnosti subiektiv systemy protydii kiberzlochynnosti. Nauka i pravookhorona. 2024. № 1(63). S.133-141. DOI: https://doi.org/10.36486/np.2024.1(63).13

25. Cooperative Cyber Defence Centre of Excellence (CCDCOE). NATO. URL: https://ccdcoe.org

26. Tiirmaa-Klaar H. (2016). Building national cyber resilience and protecting critical information infrastructure. Journal of Cyber Policy. Vol. 1, No. 1. P. 94–106.

27. Fediienko O.P. Mizhnarodni standarty otsinky kiberstiikosti. Informatsiia i pravo. 2024. № 3(50) S. 124-135. DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311680(in Ukrainian)

28.NATO's Readiness Action Plan. Strategic Benefits and Outstanding Challenges. URL: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-10_Issue-1/Arnold.pdf

29.Veselova L.Iu. Kibernetychna bezpeka v umovakh hibrydnoi viiny: administratyvno-pravovi zasady: monohrafiia. Odesa: Vydavnychyi dim «Helvetyka». 2020. 488 c. (in Ukrainian)

30. NATO Defence Ministers agree to enhance collective defence and deterrence. URL: https://www.nato.int/cps/en/natohq/news_132356.htm?selectedLocale=en

31.Herrington L., Aldrich R. (2013).The Future of Cyber-Resilience in an Age of Global Complexity. Politics. Vol. 33(4). P. 299–310.

32. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union. URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj

33.EU Cyber Resilience Act: Briefing. European Parliamentary Research Service. 2024. 12 p. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf

34. The Cyber Resilience Act: Summary of the legislative text. An official website of the European Union.URL: https://digital-strategy.ec.europa.eu/en/policies/cra-summary

35. Overview EU Cyber Resilience Act. ABB. 2024. 5 p. URL: https://library.e.abb.com/public/c87c6a5acc7443e19a6ed0e4c72d314b/9AKK108471A6145_en_A_Cybersecurity%20Guide%20EU%20CRA.pdf?x-sign=ItWWeq6GekkG8yFqPKIx87Bt%2BNxMtBWxIZYsabwKnmJgnQEwM8sYWMEd6ZJt21Lv

36. The NIS2 Directive: A high common level of cybersecurity in the EU. 2023. 13 p. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

37. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

38. European Union Cyber Resilience Act: A Compliance Guide for Connected Devices. DigiCert. 2025. 8 p. URL: https://www.digicert.com/content/dam/digicert/pdfs/whitepaper/digicert-eu-cra-whitepaper-en.pdf

39. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu

40. Computer Security Incident Response Team (CSIRT). URL: https://www.csirt.org/

41. Cyber Shield .URL: https://www.cybershield.krd/home

42.Cybersecurity and Infrastructure Security Agency (CISA). Official Website. URL: https://www.cisa.gov

43. Executive Order 14028 on Improving the Nation's Cybersecurity. The White House, 2021. URL: https://www.govinfo.gov/content/pkg/DCPD-202100401/pdf/DCPD-202100401.pdf

44. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST / Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Special Publication 800-160, Vol. 2. 2021. 294 p. DOI: https://doi.org/10.6028/NIST.SP.800-160v2r1

45. National Cyber Security Centre. URL: https://www.ncsc.gov.uk

46. The Strategic Framework for a Cyber Resilient Scotland. Scottish Government. 2021. 39 p. URL: https://dera.ioe.ac.uk/id/eprint/37463/1/strategic-framework-cyber-resilient-scotland%20%28redacted%29.pdf

47. Wilding N. (2016). Cyber resilience: How important is your reputation? How effective are your people? Business Information Review. Vol. 33, No. 2. P. 94–99.

48. Reznikova O.O. Zabezpechennia stiikosti derzhavy i suspilstva do terorystychnoi zahrozy v Ukraini ta sviti. Stratehichni priorytety. 2017. № 3 (44). C. 22-28. (in Ukrainian)

49. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 26 travnia 2015 r. №287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015(in Ukrainian)

50. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 r. «Pro Stratehiiu natsionalnoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 14 veresnia 2020 r. №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text(in Ukrainian)

51. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 26 serpnia 2021 roku № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text(in Ukrainian)

Authors Contribution: All authors have contributed equally to this work
Conflict of Interest: The authors declare no conflict of interest

The article was received by the editors 02.03.2026 The article was revised 06.04.2026
The article is recommended for printing 20.05.2026 This article published 30.05.2026