АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 347.77:004.056
DOI https://doi.org/10.32782/TNU-2707-0581/2026.5/20

Гнедюк В. Л.
https://orcid.org/0009-0007-8025-0876
Служба безпеки України

КІБЕРСТІЙКІСТЬ (ЮРИДИЧНІ АСПЕКТИ)

Стаття є дослідженням сучасного стану та тенденцій розвитку правового регулювання кіберстійкості в Україні з урахуванням відповідних підходів Європейського Союзу. Автором розкрито правову природу кіберстійкості як міжгалузевої правової категорії, що охоплює питання кібербезпеки, захисту критичної інфраструктури, управління кіберризиками, реагування на кіберінциденти та забезпечення безперервності функціонування цифрових систем. Проаналізовано нормативно-правові засади забезпечення кіберстійкості в Україні, зокрема положення законодавства у сфері кібербезпеки, критичної інфраструктури, захисту державних інформаційних ресурсів, реагування на кіберінциденти та оцінювання стану кіберзахисту. Висвітлено основні напрями розвитку національного правового регулювання у 2022–2026 роках та визначено його ключові проблеми, пов'язані з відсутністю цілісної нормативної конструкції кіберстійкості, необхідністю подальшого вдосконалення механізмів управління кіберризиками, повідомлення про кіберінциденти та відповідальності відповідних суб'єктів. Окрему увагу приділено правовому регулюванню кіберстійкості в Європейському Союзі, зокрема підходам, закріпленим у Директиві (ЄС) 2022/2555, Директиві (ЄС) 2022/2557, Регламенті (ЄС) 2022/2554 та Регламенті (ЄС) 2024/2847. Встановлено, що європейська модель характеризується переходом до ризик-орієнтованого управління, посиленням ролі органів управління, розвитком механізмів реагування та відновлення, а також поширенням вимог кібербезпеки на критичних суб'єктів і цифрові продукти. На цій основі визначено напрями подальшого вдосконалення українського законодавства з урахуванням acquis Європейського Союзу, зокрема щодо нормативного визначення кіберстійкості, удосконалення процедур повідомлення про кіберінциденти, посилення відповідальності органів управління та розвитку механізмів тестування і координованого розкриття вразливостей.

Ключові слова: *кіберстійкість, кіберризики, критична інфраструктура, кіберінцидент, кіберзахист, цифрова стійкість, acquis Європейського Союзу.*

Постановка проблеми. Стрімке зростання кіберзагроз та залежності держави і суспільства від цифрової та критичної інфраструктури зумовлює необхідність переходу від переважно захисної моделі кібербезпеки до комплексного забезпечення кіберстійкості. Для України ця проблема особливо загострилася в умовах повномасштабної збройної агресії російської федерації та систематичних кібератак на державні інформаційні ресурси й об'єкти критичної інфраструктури. Водночас розвиток законодавства у сфері кібербезпеки та захисту критичної інфраструктури не усуває проблеми системності правового регулювання та належного розмежування понять кібербезпеки, кіберзахисту і кіберстійкості. Це зумовлює необхідність визначення правової природи кіберстійкості, оцінювання стану її нормативного забезпечення в Україні та визначення напрямів його вдосконалення з урахуванням acquis Європейського Союзу.

© Гнедюк В. Л., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

Аналіз останніх досліджень і публікацій. Проблематика кіберстійкості в українській науковій літературі перебуває на етапі активного формування та концептуалізації, що зумовлено трансформацією підходів до забезпечення кібербезпеки в умовах ускладнення кіберзагроз. Важливе теоретико-правове значення має праця О. Є. Користіна та С. В. Демедюка, у якій кіберстійкість розглядається як здатність протистояти кіберризикам, відновлюватися після їх реалізації та адаптуватися до нових загроз [6]. Комплексний розвиток правової та кримінологічної проблематики здійснено С. В. Демедюком у докторській дисертації «Організаційно-правові та кримінологічні засади кіберстійкості в Україні» (2026 року), присвяченій правовому регулюванню кіберстійкості, управлінню ризиками, інституційним механізмам та її взаємозв'язку з національною безпекою і захистом критичної інфраструктури [1]. Окремі аспекти кіберстійкості у контексті національної безпеки, ідентифікації кіберризиків та посилення стійкості інформаційної інфраструктури досліджено С. В. Онищенко, А. Д. Глушко та О. А. Маслій [9]. Питання глобальних кіберзагроз, управління ризиками, моніторингу рівня кібербезпеки та захисту підприємств і критичної інфраструктури розглянуто у праці Л. В. Рибальченко, О. А. Габорець та Д. І. Прокопович-Ткаченко [22]. Правовий та кримінологічний вимір проблематики доповнює дослідження А. А. Олійник, присвячене взаємозв'язку кіберстійкості, прав людини та міжнародних превентивних моделей у цифровому просторі України [8]. Водночас, потребують подальшого дослідження системні питання правового регулювання кіберстійкості в Україні.

Постановка завдання. Метою статті є дослідження правового регулювання кіберстійкості в Україні та Європейському Союзі, виявлення основних проблем національного регулювання та визначення напрямів його вдосконалення з урахуванням acquis ЄС.

Для досягнення мети визначено такі завдання:

1. Визначити правову природу кіберстійкості та її співвідношення з кібербезпекою і кіберзахистом.

2. Проаналізувати правове регулювання кіберстійкості в Україні та ЄС.

3. Виявити основні проблеми національного регулювання та запропонувати напрями його вдосконалення.

Виклад основного матеріалу. У сучасному правовому дискурсі кіберстійкість формується як міжгалузева правова категорія, що охоплює не лише захист інформаційних систем, а й здатність відповідних суб'єктів та інфраструктури протистояти кіберзагрозам, забезпечувати безперервність функціонування та відновлюватися після кіберінцидентів. Її правове забезпечення охоплює відносини у сфері кібербезпеки, захисту критичної інфраструктури, управління кіберризиками, реагування на кіберінциденти та відповідальності. У цьому контексті розвиток правового регулювання характеризується переходом до ризик-орієнтованого управління кібербезпекою та посиленням ролі органів управління відповідних суб'єктів.

Національно-правове регулювання кібербезпеки та кіберстійкості України ґрунтується на Конституції України [5] та системі спеціального законодавства у сфері кібербезпеки, захисту критичної інфраструктури, електронних комунікацій і захисту інформації. Базовим спеціальним актом у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [19]. Водночас чинне законодавство вже пов'язує кіберзахист із забезпеченням стійкості, однак питання кіберстійкості не сформоване в законодавстві як окрема цілісна правова конструкція. Водночас розвиток відповідного нормативного регулювання продовжується, зокрема шляхом розширення механізмів реагування та обміну інформацією про кіберзагрози. Суттєвим етапом такого розвитку стало прийняття Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» від 27 березня 2025 року № 4336-IX, яким, зокрема, Закон № 2163-VIII доповнено статтею 9-1 «Національна система обміну інформацією про кіберінциденти, кібератаки, кіберзагрози» [10]. Відповідно до оновленого законодавства, Державну службу спеціального зв'язку та захисту інформації України визначено уповноваженим органом, що забезпечує функціонування зазначеної системи, а також встановлено правові засади обов'язкового і добровільного обміну інформацією про кіберінциденти, кібератаки та кіберзагрози [10]. Подальша нормативна конкретизація відповідного механізму відбулася у 2026 році: наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14 травня 2026 року № 351, зареєстрованим у Міністерстві юстиції України 22 червня 2026 року за № 899 / 46293, затверджено Порядок обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та Критерії визначення

значного кіберінциденту [15]. Окремим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 5 березня 2026 року № 179, зареєстрованим у Міністерстві юстиції України 7 квітня 2026 року за № 473 / 45867, затверджено Порядок ведення репозитарію інформації про кіберінциденти, що визначає організаційні та правові засади формування і ведення відповідного інформаційного ресурсу [14]. Отже, сучасний розвиток національного законодавства характеризується переходом від загального нормативного визначення засад кібербезпеки до деталізованого правового регулювання інформаційної взаємодії щодо кіберінцидентів, кібератак і кіберзагроз, що створює нормативне підґрунтя для підвищення спроможності держави своєчасно виявляти загрози, координувати реагування та забезпечувати кіберстійкість відповідних інформаційних і критичних систем.

Важливим самостійним напрямом розвитку національного нормативно-правового регулювання стало формування комплексного правового режиму критичної інфраструктури на основі Закону України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX, який визначає правові, організаційні та економічні засади функціонування і захисту критичної інфраструктури, а також забезпечення її стійкості [18]. Подальший розвиток зазначеного правового режиму відбувався, зокрема, шляхом внесення змін Законом України «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України» від 18 жовтня 2022 року № 2684-IX, прийнятим в умовах повномасштабної збройної агресії російської федерації [11]. Водночас механізми ідентифікації та категоризації об'єктів критичної інфраструктури врегульовано постановою Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інфраструктури», яка неодноразово зазнавала змін та на сьогодні діє у редакції від 22 травня 2026 року [3].

Окремий нормативний блок становлять акти, спрямовані безпосередньо на забезпечення кіберзахисту критичної інфраструктури, зокрема постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури», яка встановлює організаційно-методологічні засади здійснення відповідних заходів [12]. Важливе значення для формування правового розуміння кіберстійкості має постанова Кабінету Міністрів України від 11 листопада 2020 року № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом», якою безпосередньо визначено поняття «кіберстійкість критичної інформаційної інфраструктури» як стан, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз [17]. Зазначене свідчить про поступове формування в українському законодавстві окремого нормативного напряму, у межах якого кіберзахист критичної інфраструктури поєднується із забезпеченням її функціональності, безперервності роботи, відновлюваності та стійкості.

Окремий нормативний напрям розвитку правового регулювання кіберстійкості становить забезпечення функціональної стійкості державних інформаційних ресурсів та публічних електронних реєстрів в умовах воєнного стану. Важливе значення у цьому контексті має Закон України «Про хмарні послуги» від 17 лютого 2022 року № 2075-IX, який визначає правові відносини у сфері надання хмарних послуг та встановлює особливості їх використання органами державної влади, органами місцевого самоврядування, державними підприємствами, установами й організаціями та іншими визначеними законом суб'єктами, зокрема для обробки державних інформаційних ресурсів [21]. Безпосереднім правовим механізмом забезпечення функціонування інформаційно-комунікаційних систем і публічних електронних реєстрів в умовах воєнного стану стала постанова Кабінету Міністрів України від 12 березня 2022 року № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану». Зазначена постанова передбачає, зокрема, можливість розміщення державних інформаційних ресурсів та публічних електронних реєстрів на хмарних ресурсах та/або в центрах обробки даних за межами України, а також створення резервних копій відповідних інформаційних ресурсів, що спрямовано на забезпечення їх збереження та безперервності функціонування в умовах воєнного стану [2]. Таким чином, нормативне регулювання функціонування державних цифрових ресурсів у воєнний період доповнює традиційні механізми кіберзахисту інструментами резервування, дублювання та використання розподіленої інфраструктури, що має безпосереднє значення для забезпечення

їх функціональної стійкості та відновлення у разі порушення штатного режиму роботи.

Стратегічний рівень правового регулювання представлений Стратегією кібербезпеки України, затвердженою Указом Президента України від 26 серпня 2021 року № 447 / 2021, яка визначає забезпечення кібербезпеки одним із пріоритетів у системі національної безпеки України та орієнтує державну політику на посилення спроможностей національної системи кібербезпеки і досягнення кіберстійкості на всіх рівнях [20]. Подальше нормативне забезпечення механізмів реагування на кіберзагрози було розвинуте постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози», якою затверджено, зокрема, Національний план реагування на кіберінциденти, кібератаки та кіберзагрози, а також визначено відповідні організаційні засади реагування та інформаційної взаємодії [4]. На рівні оцінювання стану кіберзахисту важливим етапом розвитку нормативної бази стало прийняття постанови Кабінету Міністрів України від 31 грудня 2025 року № 1799 «Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури», яка встановлює механізм проведення такого оцінювання та визначає його основні види [16].

Секторальний рівень регулювання найбільш комплексно представлений у фінансовому секторі, де Національний банк України сформував спеціальну нормативну систему забезпечення кіберзахисту банківської системи. Ключовим актом у цій сфері є постанова Правління Національного банку України від 12 серпня 2022 року № 178 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України», якою затверджено Положення про організацію кіберзахисту в банківській системі України та визначено основні організаційні засади забезпечення кіберзахисту в банківській системі [13]. Зазначене регулювання надалі розвивалося шляхом внесення змін, зокрема постановою Правління НБУ від 25 лютого 2025 року № 24 «Про затвердження Змін до деяких нормативно-правових актів Національного банку України з питань інформаційної безпеки та кіберзахисту», постановою від 27 червня 2025 року № 69 «Про критичну інфраструктуру фінансового сектору» та постановою від 12 червня 2026 року № 66.

Правове регулювання кіберстійкості в Європейському Союзі сформовано як багаторівневу систему, що охоплює управління кіберризиками, стійкість критичних суб'єктів, цифрову операційну стійкість фінансового сектору та безпеку продуктів із цифровими елементами. Директива (ЄС) 2022/2555 Європейського Парламенту і Ради від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки в Союзі (NIS2) встановлює вимоги до управління кіберризиками, запобігання та реагування на кіберінциденти, забезпечення безперервності діяльності, а також передбачає відповідальність органів управління відповідних суб'єктів за затвердження та контроль заходів з управління кіберризиками [23]. Директива (ЄС) 2022/2557 Європейського Парламенту і Ради від 14 грудня 2022 року про стійкість критичних суб'єктів (CER) встановлює правові засади забезпечення спроможності критичних суб'єктів запобігати інцидентам, протистояти їм, реагувати на них, відновлюватися після їх настання та забезпечувати безперервність надання основних послуг [24]. Спеціальний режим для фінансового сектору встановлено Регламентом (ЄС) 2022/2554 Європейського Парламенту і Ради від 14 грудня 2022 року про цифрову операційну стійкість фінансового сектору (DORA), який регулює управління ІКТ-ризиками, повідомлення та реагування на ІКТ-інциденти, тестування цифрової операційної стійкості та ризики, пов'язані з ІКТ-послугами третіх сторін [25]. Окремий горизонтальний рівень становить Регламент (ЄС) 2024/2847 Європейського Парламенту і Ради від 23 жовтня 2024 року про горизонтальні вимоги кібербезпеки для продуктів із цифровими елементами (Cyber Resilience Act), який встановлює вимоги до кібербезпеки таких продуктів на етапах їх проєктування, розроблення, виробництва та протягом життєвого циклу, включаючи управління вразливостями [26]. Водночас стандарти ISO/IEC 27001, ISO 22301 та NIST Cybersecurity Framework 2.0 мають методологічне значення для управління інформаційною безпекою, забезпечення безперервності діяльності та управління кіберризиками, проте самі по собі не є актами права Європейського Союзу. Таким чином, європейська нормативна модель характеризується переходом від фрагментарного регулювання окремих аспектів кібербезпеки до комплексного правового забезпечення управління кіберризиками, відповідальності органів управління, реагування

та відновлення, безперервності функціонування, стійкості критичних суб'єктів і безпеки цифрових продуктів, що визначає важливі напрями подальшого наближення законодавства України до acquis Європейського Союзу.

Забезпечення кіберстійкості передбачає застосування комплексу юридичних засобів, спрямованих як на запобігання порушенням у сфері кібербезпеки, так і на притягнення винних осіб до відповідальності. Кримінально-правовий захист забезпечується положеннями розділу XVI Особливої частини Кримінального кодексу України, який охоплює, зокрема, кримінальні правопорушення, пов'язані з несанкціонованим втручанням у роботу інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, створенням і поширенням шкідливих програмних чи технічних засобів, несанкціонованими діями з інформацією та іншими посяганнями на безпеку інформаційних систем [7]. Адміністративно-правові засоби застосовуються у випадках порушення встановлених законодавством вимог у сфері захисту інформації та кібербезпеки, якщо за відповідне діяння законом передбачено адміністративну відповідальність.

Водночас у праві Європейського Союзу простежується тенденція до посилення відповідальності органів управління за управління кіберризиками. Так, відповідно до статті 20 Директиви (ЄС) 2022/2555 (NIS2) органи управління основних та важливих суб'єктів зобов'язані затверджувати заходи з управління кіберризиками та здійснювати нагляд за їх реалізацією, а держави-члени повинні забезпечити можливість притягнення членів таких органів до відповідальності за порушення відповідних вимог згідно з національним законодавством. У фінансовому секторі цей підхід отримав подальший розвиток у статті 5 Регламенту (ЄС) 2022/2554 (DORA), відповідно до якої орган управління фінансової установи несе кінцеву відповідальність за управління ІКТ-ризиками, затверджує відповідну систему управління та здійснює нагляд за її реалізацією.

Висновки. Отже, правове регулювання кіберстійкості в Україні формується як міжгалузевий комплекс норм у сфері кібербезпеки, захисту критичної інфраструктури, управління кіберризиками та реагування на кіберінциденти. Водночас його подальший розвиток потребує чіткішого нормативного визначення кіберстійкості та наближення окремих механізмів до підходів acquis ЄС.

Основними напрямами вдосконалення є:

1. Удосконалення понятійного апарату – нормативно визначити поняття «кіберстійкість» та узгодити його з категоріями кібербезпеки і кіберзахисту.

2. Удосконалення повідомлення про кіберінциденти – наблизити національні процедури до диференційованих моделей NIS2 та CRA і забезпечити єдиний механізм подання повідомлень.

3. Посилення ролі органів управління – закріпити їх обов'язки щодо управління кіберризиками, нагляду та підвищення відповідної компетентності з урахуванням NIS2 і DORA.

4. Розвиток тестування та розкриття вразливостей – запровадити регулярні навчання з реагування на кіберінциденти та нормативно врегулювати механізми координованого повідомлення про вразливості.

Список літератури:

1. Демедюк С. В. Організаційно-правові та кримінологічні засади кіберстійкості в Україні : дис. ... д-ра юрид. наук : 12.00.07 ; 12.00.08. Одеса. 2026. 525 с.

2. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану : Постанова Каб. Міністрів України від 12.03.2022 № 263. URL: https://zakon. rada.gov.ua/laws/show/263–2022-п#Text (дата звернення: 13.08.2026).

3. Деякі питання об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 09.10.2020 № 1109. URL: https://zakon. rada.gov.ua/laws/show/1109–2020-п#Text (дата звернення: 13.08.2026).

4. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Каб. Міністрів України від 26.11.2025 № 1533. URL: https://zakon. rada.gov.ua/laws/show/1533–2025-п#Text (дата звернення: 15.08.2026).

5. Конституція України : від 28.06.1996 № 254к/96-ВР. URL: https://zakon. rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 13.08.2026).

6. Користін О. Є., Демедюк С. В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство.* 2023. № 6. С. 708–713.

7. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III. URL: https://zakon. rada.gov.ua/laws/show/2341–14#Text (дата звернення: 15.08.2026).

8. Олійник А. А. Кіберстійкість та права людини: імплементація міжнародних превентивних моделей у цифровий простір в Україні. *Аналітично-порівняльне правознавство*. 2025. Т. 3, № 6. С. 84–90.

9. Онищенко С. В., Глушко А. Д., Маслій О. А. Кіберстійкість як основа національної безпеки України. *Innovations and prospects of world science* : Proceedings of XI International Scientific and Practical Conference, Vancouver, Canada, 22–24 June 2022. Vancouver : Perfect Publishing, 2022. С. 551–556.

10. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon. rada.gov.ua/laws/show/4336–20#Text (дата звернення: 14.08.2026).

11. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України : Закон України від 18.10.2022 № 2684-IX. URL: https://zakon. rada.gov.ua/laws/show/2684–20#Text (дата звернення: 13.08.2026).

12. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19.06.2019 № 518. URL: https://zakon. rada.gov.ua/laws/show/518–2019-п#Text (дата звернення: 13.08.2026).

13. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України : Постанова Нац. банку України від 12.08.2022 № 178. URL: https://zakon. rada.gov.ua/laws/show/v0178500–22#Text (дата звернення: 15.08.2026).

14. Про затвердження Порядку ведення репозитарію інформації про кіберінциденти : Наказ Адмін. Держ. служби спец. зв'язку та зах. інформації України від 05.03.2026 № 179. URL: https://zakon. rada.gov.ua/laws/show/z0473–26#Text (дата звернення: 14.08.2026).

15. Про затвердження Порядку обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та Критеріїв визначення значного кіберінциденту : Наказ Адмін. Держ. служби спец. зв'язку та зах. інформації України від 14.05.2026 № 351. URL: https://zakon. rada.gov.ua/laws/show/z0899–26#Text (дата звернення: 14.08.2026).

16. Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури : Постанова Каб. Міністрів України від 31.12.2025 № 1799. URL: https://zakon. rada.gov.ua/laws/show/1799–2025-п#Text (дата звернення: 15.08.2026).

17. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : Постанова Каб. Міністрів України від 11.11.2020 № 1176. URL: https://zakon. rada.gov.ua/laws/show/1176–2020-п#Text (дата звернення: 12.08.2026).

18. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon. rada.gov.ua/laws/show/1882–20#Text (дата звернення: 12.08.2026).

19. 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 (дата звернення: 12.08.2026).

20. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon. rada.gov.ua/laws/show/447/2021#Text (дата звернення: 15.08.2026).

21. Про хмарні послуги : Закон України від 17.02.2022 № 2075-IX. URL: https://zakon. rada.gov.ua/laws/show/2075–20#Text (дата звернення: 14.08.2026).

22. Рибальченко Л. В., Габорець О. А., Прокопович-Ткаченко Д. І. Кіберстійкість: глобальні загрози та національні стратегії кіберзахисту. *Системи та технології.* 2024. Т. 68, № 2. С. 95–101.

23. 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). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (дата звернення: 15.08.2026).

24. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. URL: https://eur-lex. europa. eu/eli/dir/2022/2557/oj/eng (дата звернення: 15.08.2026).

25. 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/eng (дата звернення: 15.08.2026).

26. 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). URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng (дата звернення: 15.08.2026).

Gnediuk V. L. CYBER RESILIENCE (LEGAL ASPECTS)

The article examines the current state and development trends of the legal regulation of cyber resilience in Ukraine, taking into account the relevant approaches of the European Union. The author elucidates the legal nature of cyber resilience as an interdisciplinary legal category encompassing cybersecurity, critical infrastructure protection, cyber risk management, cyber incident response, and ensuring the continuity of digital systems. The article analyses the regulatory framework for ensuring cyber resilience in Ukraine, including legislation on cybersecurity, critical infrastructure, protection of state information resources, cyber incident response, and assessment of cybersecurity. Particular attention is paid to the main directions of development of national legal regulation in 2022–2026 and to the key challenges arising from the absence of a comprehensive legal framework for cyber resilience, as well as the need to further improve mechanisms for cyber risk management, cyber incident reporting, and liability of relevant entities. The study also examines the legal regulation of cyber resilience in the European Union, with particular emphasis on the approaches established by Directive (EU) 2022/2555, Directive (EU) 2022/2557, Regulation (EU) 2022/2554, and Regulation (EU) 2024/2847. It is established that the European regulatory model is characterised by a shift towards risk-based management, enhanced responsibilities of management bodies, development of response and recovery mechanisms, and the extension of cybersecurity requirements to critical entities and products with digital elements. On this basis, the article identifies directions for further improvement of Ukrainian legislation in accordance with the EU acquis, including the legal definition of cyber resilience, improvement of cyber incident reporting procedures, strengthening the responsibility of management bodies, and development of mechanisms for resilience testing and coordinated vulnerability disclosure.

Keywords: *cyber resilience, cyber risks, critical infrastructure, cyber incident, cybersecurity, digital resilience, EU acquis.*

Дата першого надходження статті до видання: 24.08.2026
Дата прийняття статті до друку після рецензування: 07.09.2026
Дата публікації (оприлюднення) статті: 18.11.2026