



Правове забезпечення резильєнтності критичної інфраструктури міст України

Роман КІРІН,

доктор юридичних наук, доцент, провідний науковий співробітник,
Державна установа «Інститут економіко-правових досліджень
імені В. К. Мамутова Національної академії наук України» (м. Київ),
ORCID [0000-0003-0089-4086](https://orcid.org/0000-0003-0089-4086), e-mail: kirins62@gmail.com.

Анотація. Досліджуються актуальні питання правового забезпечення резильєнтності критичної інфраструктури міст України. Аргументується, що специфіка формування та розвитку інституту законодавства про критичну інфраструктуру полягає в тому, що базовий закон регулює відносини у сфері функціонування та захисту критичної інфраструктури в цілому та її об'єктів у мирний час. Розкривається міжгалузевий характер інституту законодавства про критичну інфраструктуру, що містить приписи, які віднесені до блоків законодавства про національну безпеку і оборону України, основи містобудування, забезпечення діяльності транспорту, забезпечення діяльності зв'язку, місцеве самоврядування в Україні, громадські об'єднання, охоронну діяльність, інформацію тощо. Запропоновано узгодити приписи ст. 25 Закону України «Про критичну інфраструктуру» з положеннями Закону України «Про публічно-приватне партнерство». Крім того, в чинній редакції базового закону відсутні кореляційні положення щодо Закону України «Про концесію». Визначено напрями резильєнтності критичної інфраструктури міст України, що першочергово потребують правового врегулювання: енергетичний сектор, водопостачання та водовідведення, охорона здоров'я, транспорт та логістика, телекомунікації та ІТ, стійкість органів місцевого самоврядування, цивільний захист, міграційна та демографічна стійкість, стійкість мешканців міста, фінансово-економічна стійкість. Обліковано підзаконний блок законодавства, що безпосередньо пов'язаний із базовим законом про критичну інфраструктуру, а також частину нормативно-правових актів, які не згадуються в Законі України «Про критичну інфраструктуру», але регулюють відносини у цій сфері. Виокремлюються базові цілі в контексті правового забезпечення резильєнтності об'єктів критичної інфраструктури міст України. Встановлюється багатоаспектний зв'язок між категоріями «відкритість міста» та «захист критичної інфраструктури». Ключовими аспектами взаємодії вказаних понять є захист критичної технологічної інформації, інформаційна та кібербезпека, прозорість закупівель і тендерів, управління ризиками та комунікація, а також залучення громадян.

Ключові слова: національна безпека, облік законодавства, місцеве самоврядування, нормативно-правові акти, захист, стійкість.

Надійшла: 17.07.2026. Прийнята: 02.09.2026. Опублікована онлайн: 23.09.2026. Надрукована: 30.10.2026

© Кірін Р., 2026

Ліцензія відкритого доступу: [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)



Постановка проблеми

Об'єкти критичної інфраструктури (далі — ОКІ), виходячи із положень чинного Закону України «Про критичну інфраструктуру» [1] (далі — Закон про КІ), володіють такими ознаками:

- а) структура — об'єкти інфраструктури, системи, їхні частини та їхня сукупність;
- б) значення — важливість для економіки, національної безпеки та оборони;
- в) необхідність охорони — порушення їх функціонування може завдати шкоди життєво важливим національним інтересам.

Для міст України ОКІ, по суті, є системою їх життєзабезпечення, від якої залежать виживання, безпека та економіка в умовах повномасштабної війни. Вона забезпечує базові потреби містян та міського середовища, як-от: тепло-, енерго-, водопостачання, медицину та зв'язок.

На державному рівні здійснюється постійне фінансування захисту і відновлення ОКІ, а також оптимізація цих процесів. Резильєнтність (стійкість) роботи підприємств, що обслуговують ОКІ, підтримується спеціальним статусом, який регламентовано згаданим вище законом про КІ. Крім того, держава запроваджує Комплексні плани стійкості регіонів та окремих міст [2], а також оновлює критерії для оперативного бронювання працівників, залучених до відновлення та захисту ОКІ. Тож правове забезпечення стійкості ОКІ міст слід розглядати як один із юридичних елементів фундаменту національної безпеки України. Саме воно визначає загальні положення, основні засади державної політики у сфері захисту ОКІ, їхній правовий статус, національну систему захисту та її організаційні засади, об'єктний і суб'єктний склади відповідних правовідносин, а також встановлює обов'язки для бізнесу, держави, регіонів та міст щодо алгоритмів швидкого відновлення ОКІ. За цих умов дослідження правового забезпечення резильєнтності КІ міст України уявляється надзвичайно актуальним та своєчасним науково-практичним напрямом.

Аналіз останніх досліджень та публікацій

Тематика, обрана для дослідження, в силу своєї важливості та комплексного характеру є предметом зацікавленості міжгалузевої спільноти науковців з різних дослідницьких кластерів. Зокрема, з економіко-правових позицій були опрацьовані питання забезпечення стійкості КІ в Україні в умовах сучасних викликів [3]. Автор слушно відмічає, що серед найбільш важливих складників, що впливають на стійкість КІ, є розвиток технологій кібербезпеки, адекватність правових норм та здатність до адаптації КІ до нових загроз. У дослідженні, присвяченому сучасному стану та напрямам удосконалення системи правового регулювання захисту ОКІ в Україні [4, с. 182], вказується, що через порушення послідовності дій суб'єктів та основний принцип «від загального до окремого (до складових)» під час формування в Україні національного законодавства про КІ основний закон, що регулює діяльність у сфері захисту КІ, має певні розбіжності між положеннями, які містяться в ньому; неточностями у визначеннях і поняттях, які були сформовані раніше у певних НПА в галузях і секторах, які є відповідними складниками КІ та мають бути частиною правового регулювання, зокрема, у сфері кібербезпеки та не нести протиріч і непорозумінь.

Організаційні аспекти забезпечення безпеки і стійкості КІ України детально розглянуті в колективній аналітичній доповіді вчених Національного інституту стратегічних досліджень [5], проте правові аспекти були досліджені лише в обмеженому форматі щодо засади формування вимог до захисту ОКІ.



Питання державної політики у сфері захисту КІ під час дії воєнного стану [6] розглядала Б. Богдан. У межах поставленої мети авторкою також проаналізовано низку нормативно-правових та підзаконних актів, норми яких спрямовані на забезпечення безпеки КІ, серед яких — Національний план захисту та забезпечення безпеки та стійкості КІ, Порядок проведення моніторингу рівня безпеки ОКІ, Методика та критерії і показники оцінки стану захищеності ОКІ. Втім, очевидно, що цей перелік є неповним.

На думку К. Ковальова, який вивчав сучасні виклики та загрози для КІ України під час воєнного стану [7], є необхідність реформування законодавчої бази та посилення координації між державним і приватним секторами, хоча пропозиції в цьому напрямі автор так і не навів.

Окремі аспекти стійкості КІ були розглянуті й у статтях зарубіжних дослідників. Стійкість КІ в Україні (енергетика, транспорт та зв'язок) стала предметом висвітлення у звіті щодо ризиків та стійкості, підготовленому на замовлення Швейцарського федерального управління цивільного захисту (FOCP) з метою аналізу інформації, опублікованої на сьогодні щодо наслідків та заходів із забезпечення стійкості українських ОКІ після російського вторгнення, а також визначення попередніх висновків щодо захисту та стійкості ОКІ в умовах війни. Аналіз ОКІ крізь призму нещодавно прийнятої Директиви ЄС 2022/2557 щодо критично важливих об'єктів, яка визначає стійкість як здатність запобігати інцидентам, захищатися від них, реагувати на них, протистояти їм, пом'якшувати їхні наслідки, поглинати їх, пристосовуватися до них та відновлюватися після них, дозволяє виявити характеристики, фактори та заходи, які сприяли підвищенню стійкості ОКІ України. На думку експертів, з якою варто погодитися, належне законодавство сприяє забезпеченню готовності ОКІ [8].

Китайські науковці навели дані за різними сценаріями та аналіз конкретного випадку щодо оцінки стійкості ОКІ на основі цілісного та теоретичного підходу [9]. Ними запроваджено новий, екологічно орієнтований підхід до оцінки стійкості КІ, який отримав назву «Нова крива оцінки стійкості інфраструктури» (NIRAC).

Представники польської платформи з питань національної безпеки представили значення науково-дослідних проєктів ЄС у сфері захисту КІ [10]. Акцентовано увагу на Директиві (ЄС) 2022/2557 від 14 грудня 2022 р. щодо стійкості критично важливих суб'єктів, Директиві (ЄС) 2022/2555 від 14 грудня 2022 р. щодо заходів для забезпечення високого спільного рівня кібербезпеки в усьому Союзі та Рекомендації Ради від 25 червня 2024 р. щодо плану координації заходів реагування на рівні Союзу на випадки порушення функціонування КІ, що мають значне транскордонне значення. На жаль, нині проєкт закону щодо імплементації положень вказаних європейських актів з 08 листопада 2024 р. перебуває у стадії ознайомлення.

Варто також відзначити й попередні, загальнотеоретичні та вузькоспецифічні підходи до проблем міської стійкості, які висвітлювали правове забезпечення комплексної резильєнтності міст України [11], цифрові та правові виміри інноваційної складової резильєнтності міста [12] тощо.

Проте говорити про науково-практичну вичерпаність обраної проблематики, очевидно, зарано. Нові виклики потребують системного підходу до чинного законодавства в обраній сфері. Незважаючи на наявність цих та багатьох інших публікацій, що торкалися правових проблем стійкості КІ, окремі питання не були піддані комплексному аналізу та все ще мають достатній дослідницький потенціал.



Мета дослідження

Метою роботи є виявлення та облік законодавства у сфері забезпечення стійкості об'єктів критичної інфраструктури міст України як складового блоку законодавства про національну систему стійкості.

Виклад основного матеріалу дослідження

Специфіка формування та розвитку інституту законодавства про КІ полягає в тому, що базовий закон про КІ регулює відносини у сфері функціонування та захисту КІ в цілому та ОКІ у мирний час. Водночас особливості захисту та правового режиму ОКІ в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду регулюються законами України про правовий режим воєнного стану, правовий режим надзвичайного стану, функціонування єдиної транспортної системи України в особливий період, оборону України. Крім того, окремим законом регулюються відносини щодо забезпечення кіберзахисту та кібербезпеки ОКІ [13], а також правові основи організації та діяльності Держспецзв'язку — Законом України «Про Державну службу спеціального зв'язку та захисту інформації України». Саме Держспецзв'язку під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування, здійснює повноваження уповноваженого органу у сфері захисту КІ України, передбачені законом про КІ.

До наведеного переліку законодавчих актів, що в суміжний спосіб регулюють відносини у сфері КІ, слід віднести й Закон України «Про національну безпеку України», в якому задекларовано, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки КІ, кібербезпеки України та на інші її напрями. Більше того, в преамбулі закону про КІ визначено, що цей закон є складником законодавства у сфері національної безпеки. Натомість інформаційно-пошуковою системою «Законодавство України» закон про КІ класифіковано як міжгалузевий, що містить приписи, які віднесені до блоків законодавства про національну безпеку та правопорядок, основи містобудування, забезпечення діяльності транспорту, забезпечення діяльності зв'язку.

Для посадових осіб суб'єктів національної системи захисту КІ, визначених законом про КІ, інформація з Реєстру ОКІ, у зв'язку із здійсненням ними повноважень, надається за суб'єктом права чи за ОКІ в електронній формі шляхом безпосереднього доступу до цього Реєстру, за умови ідентифікації відповідної посадової особи в порядку, встановленому Законом України «Про електронні довірчі послуги».

Аналіз змісту закону про КІ дав можливість виявити ще кілька законодавчих актів, які містять приписи, що стосуються КІ-відносин, — це закони про Збройні Сили України, Національну поліцію, Національну гвардію України, порядок направлення підрозділів Збройних Сил України до інших держав, порядок допуску та умови перебування підрозділів збройних сил інших держав на території України, Кабінет Міністрів України (далі — КМУ), місцеві державні адміністрації, місцеве самоврядування в Україні, громадські об'єднання, Національний банк України, банки і банківську діяльність, охоронну діяльність, інформацію, захист інформації в інформаційно-телекомунікаційних системах, доступ до публічної інформації, державну таємницю. До законодавчого КІ-блоку слід віднести й окремі приписи Кодексу України про адміністративні правопорушення (ст.ст. 61, 99, 188-36), Кримінального кодексу України (ст.ст. 259, 360) та Кодексу цивільного захисту України (ст.ст. 8, 32).



Окремо слід звернути увагу на положення ст. 25 закону про КІ щодо державно-приватного партнерства у сфері захисту КІ. По-перше, їх пропонується узгодити з положеннями Закону України «Про публічно-приватне партнерство». По-друге, в чинній редакції закону про КІ відсутні кореляційні положення щодо Закону України «Про концесію» в частині концесійного договору та інформації про ОКІ.

У контексті резильентності міських ОКІ базовий закон (ст. 20) передбачає, що місцеві органи виконавчої влади (військово-цивільні адміністрації — у разі утворення) у сфері захисту КІ забезпечують:

1) розроблення та затвердження місцевих програм забезпечення безпеки та стійкості КІ;

2) розроблення, затвердження та погодження із заінтересованими органами місцевих планів відновлення функціонування КІ.

Подібний виклад повноважень у спеціальному законі є більш конкретним, аніж той, що наведений в Законі України «Про місцеве самоврядування в Україні» (ст. 38). Останній до відання виконавчих органів міських рад відносить такі делеговані повноваження щодо забезпечення законності, правопорядку, охорони прав, свобод і законних інтересів громадян, як:

— вжиття необхідних заходів щодо захисту КІ, відновлення функціонування ОКІ;

— взаємодія між суб'єктами національної системи захисту КІ з урахуванням вимог закону про КІ.

При цьому ці повноваження були додані до муніципального законодавства лише з прийняттям закону про КІ.

Перед тим, як перейти до підзаконного блоку КІ-законодавства, варто виділити значення для міст тих КІ-складових, що першочергово потребують правового врегулювання:

1) енергетичний сектор — забезпечення електроенергією та теплом житлових будинків, суб'єктів господарювання та соціальних об'єктів; стабільна енергетика є основою для виживання міст, тому акцент робиться на розподіленій генерації та резервному живленні;

2) водопостачання та водовідведення — постачання питної води та утилізація відходів; порушення цієї системи миттєво створює загрозу санітарній та екологічній безпеці міста;

3) охорона здоров'я — лікарні та критичні медичні заклади потребують безперебійної роботи для порятунку життів та лікування поранених;

4) транспорт та логістика — залізниця, дороги, громадський транспорт є важливими для евакуації, постачання гуманітарних вантажів та функціонування економіки;

5) телекомунікації та ІТ — підтримують зв'язок, функціонування банківської сфери, управління містом та координацію рятувальних служб.

Безумовно, кожен з перерахованих напрямів має власне правове забезпечення, специфічні ОКІ, правовий статус яких визначається з урахуванням положень закону про КІ. Крім того, Концепція забезпечення Національної системи стійкості [14] передбачає функціонування таких базових елементів резильентності міст:

1) функціональна та інституційна стійкість системи органів місцевого самоврядування;



2) стійкість ОКІ (стійке водо-, енерго- та теплопостачання, оборонна та правоохоронна, медична, транспортна, продовольча, інформаційна, комунікаційна стійкість та кіберстійкість);

3) стійкість системи цивільного захисту;

4) міграційна та демографічна стійкість;

5) суспільна стійкість;

6) фінансово-економічна стійкість.

Водночас комплексні плани стійкості окремих міст [2] базуються на чотирьох ключових напрямках:

- захист ОКІ;
- розвиток розподіленої енергогенерації;
- резервне та альтернативне живлення;
- децентралізація теплогенерації.

До них слід додати й напрям безпеки та цивільного захисту (розробка планів безпеки, ОКІ-захист, створення мережі укриттів та оновлення систем оповіщення), які в сукупності мають сформувати заходи стійкості міст (*urban resilience*), тобто — ресурси, стратегії та механізми, які дозволяють міській системі витримувати критичні навантаження, швидко відновлюватися після потрясінь та адаптуватися до нових загроз [15].

До специфічних властивостей підзаконного блоку КІ-законодавства віднесемо той факт, що далеко не всі нормативно-правові акти (далі — НПА) прийняті відповідно до положень закону про КІ. Безпосередньо пов'язана із законом частина НПА регулює такі сфери та відносини щодо:

— ведення Реєстру ОКІ, включення таких об'єктів до Реєстру, доступу та надання інформації з нього (постанова Кабінету Міністрів України від 28 квітня 2023 р. № 415);

— розроблення та погодження паспорта безпеки на ОКІ (постанова Кабінету Міністрів України від 04 серпня 2023 р. № 818);

— обміну інформацією між суб'єктами національної системи захисту КІ (постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1174);

— управління ризиками безпеки на ОКІ I категорії критичності (постанова Кабінету Міністрів України від 01 квітня 2025 р. № 367);

— захисту ОКІ III та IV категорій критичності секторів громадської безпеки та цивільного захисту населення і територій (наказ Міністерства внутрішніх справ України від 17 квітня 2026 р. № 351);

— річного звіту про виконання секторальним органом та оператором КІ повноважень, визначених законом про КІ, та його форми (постанова Кабінету Міністрів України від 14 жовтня 2022 р. № 1175);

— проведення моніторингу рівня безпеки ОКІ (постанова Кабінету Міністрів України від 22 липня 2022 р. № 821);

— формування і виконання Національного плану захисту та забезпечення безпеки та стійкості КІ (розпорядження Кабінету Міністрів України від 19 вересня 2023 р. № 825-р).

Частина НПА, про які згадки у законі про КІ відсутні, але входить до системи актів, покликаних забезпечити стійкість міст, регулюючи такі сфери та відносини щодо:

— кіберзахисту ОКІ (постанова Кабінету Міністрів України від 19 червня 2019 р. № 518, у редакції постанови від 13 листопада 2025 р. № 1470);



— формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури (постанова Кабінету Міністрів України від 09 жовтня 2020 р. № 943);

— віднесення об'єктів до КІ, визначення переліку КІ-секторів, категоризації ОКІ (постанова Кабінету Міністрів України від 09 жовтня 2020 р. № 1109, у редакції постанови від 16 грудня 2022 р. № 1384, наказ Адміністрації Держспецзв'язку від 15 січня 2021 р. № 23, у редакції наказу від 26 вересня 2023 р. № 857);

— проведення зовнішнього аудиту діяльності уповноваженого органу у сфері захисту критичної інфраструктури України (постанова Кабінету Міністрів України від 10 червня 2022 р. № 675);

— реалізації експериментального проекту із створення, впровадження та забезпечення функціонування Єдиної цифрової інтегрованої інформаційно-аналітичної системи управління процесом відбудови об'єктів нерухомого майна, будівництва та інфраструктури (постанова Кабінету Міністрів України від 15 листопада 2022 р. № 1286);

— організації і порядку несення служби з охорони ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, важливих державних об'єктів, ОКІ та спеціальних вантажів Національною гвардією України (наказ Міністерства внутрішніх справ України від 15 червня 2023 р. № 497);

— організації захисту та забезпечення безпеки функціонування ОКІ та енергетики України в умовах ведення воєнних дій (рішення РНБО від 17 жовтня 2023 р., введено в дію Указом Президента України від 17 жовтня 2023 р. № 695/2023);

— єдиної цифрової інтегрованої інформаційно-аналітичної системи управління процесом відбудови об'єктів нерухомого майна, будівництва та інфраструктури (наказ Міністерства розвитку громад, територій та інфраструктури України від 23 січня 2024 р. № 65, зараз — Міністерство розвитку громад та територій України, далі — Мінрозвитку);

— формування Плану захисту ОКІ за проектною загрозою національного рівня «кібератака/кіберінцидент»; розроблення Плану захисту ОКІ за проектною загрозою національного рівня «кібератака/кіберінцидент» (наказ Служби безпеки України і Адміністрації Держспецзв'язку від 19 грудня 2024 р. № 627/772);

— оцінки стану захищеності ОКІ; застосування критеріїв і показників оцінки стану захищеності ОКІ (наказ Адміністрації Держспецзв'язку від 14 січня 2025 р. № 17);

— реалізації експериментального проекту щодо нарощування спроможностей радіоелектронного прикриття ОКІ (постанова КМУ від 15 липня 2025 р. № 881).

— проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена Законом України «Про національну безпеку України» (постанова КМУ від 11 листопада 2020 р. № 1176).

Важливе місце у формуванні КІ-законодавства щодо забезпечення стійкості ОКІ міст України відіграє Національний план захисту та забезпечення безпеки та стійкості КІ [16], цілі якого передбачають:

1) правову регламентацію діяльності суб'єктів національної системи КІ-захисту:

1.1) уточнення завдань та повноважень суб'єктів національної системи КІ-захисту;

1.2) установлення вимог та забезпечення моніторингу рівня захисту ОКІ;



2) створення системи координації та взаємодії суб'єктів національної системи КІ-захисту:

2.1) визначення порядку взаємодії під час реагування на загрози КІ та виникнення кризових ситуацій;

2.2) забезпечення функціонування системи обміну інформацією;

3) запровадження управління ризиками КІ:

3.1) періодичне проведення оцінки ризиків і загроз;

3.2) управління рівнем захисту та розвиток спроможностей реагувати на загрози;

4) посилення стійкості національної системи КІ-захисту:

4.1) посилення КІ-стійкості до функціонування у кризовій ситуації;

4.2) посилення стійкості населення до припинення надання життєво важливих функцій та/або послуг;

5) налагодження міжнародної співпраці:

5.1) взаємодія національної системи КІ-захисту з міжнародними системами.

Євроінтеграційний аспект розвитку українського КІ-законодавства, а відтак і правового забезпечення резильєнтності ОКІ міст України слід пов'язувати з актами ЄС у цій сфері, присвяченими стійкості критично важливих суб'єктів [17], заходам із забезпечення високого спільного рівня кібербезпеки на всій території ЄС [18], а також координації заходів на рівні ЄС у відповідь на порушення функціонування КІ, що мають значний транскордонний вплив [19].

Нарешті пропонується розглянути питання про поєднання відкритості міста (управління, населення і середовища) та захисту критичної інфраструктури, узгодження яких наразі становить окрему проблему [20]. Відкритість (прозорість) сприяє підзвітності та залученню учасників міської територіальної громади, а КІ-захист вимагає збереження критичної технологічної інформації в умовах війни. Міста забезпечують цей зв'язок через обмеження доступу до секретних елементів, але максимальне розкриття загальних планів, бюджетів та сервісів безпеки є корисним для управління та населення лише до межі, де воно починає описувати технічну архітектуру та вразливості міського середовища. КІ-безпека у відкритому місті досягається не засекречуванням усього, а побудовою систем, які є стійкими [21; 22].

Зв'язок між цими поняттями виражається у кількох ключових аспектах:

1) захист критичної технологічної інформації, інформаційна та кібербезпека — точні плани комунікацій, підстанцій, систем водопостачання чи медичних установ становлять державну таємницю і є закритими від публічного доступу для запобігання диверсіям та кібератакам;

2) прозорість закупівель та тендерів — громада не повинна бачити специфікацій технологій КІ-захисту (наприклад, схеми фізичної охорони або систем РЕБ), проте витрати коштів на ці потреби мають бути максимально відкритими для уникнення корупції;

3) управління ризиками та комунікація — міська влада має регулярно оцінювати безпеку своїх громад (громадську резильєнтність), водночас громадяни повинні розуміти алгоритми дій у кризових ситуаціях — куди звертатися, якщо КІ постраждала (наприклад, інформація про Пункти Незламності, мапи укриттів тощо);



4) залучення громадян — у питаннях КІ, як-от: екологічний моніторинг чи контроль за станом навколо небезпечних об'єктів, відкритість даних допомагає громадськості вчасно реагувати на потенційні загрози та контролювати дії КІ-операторів [23].

Висновки

Розгляд правового забезпечення стійкості об'єктів критичної інфраструктури міст України дав підстави для таких узагальнень.

1. Аргументовано, що специфіка формування та розвитку інституту законодавства про критичну інфраструктуру полягає в тому, що базовий закон регулює відносини у сфері функціонування та захисту критичної інфраструктури в цілому та її об'єктів у мирний час. Водночас особливості захисту та правового режиму таких об'єктів в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду регулюються законами України про правовий режим воєнного стану, правовий режим надзвичайного стану, функціонування єдиної транспортної системи України в особливий період, оборону України, забезпечення кіберзахисту та кібербезпеки, правові основи організації та діяльності Держспецзв'язку.

2. Розкрито міжгалузевий характер інституту законодавства про критичну інфраструктуру, що містить приписи, які віднесені до блоків законодавства про національну безпеку України, основи містобудування, забезпечення діяльності транспорту, забезпечення діяльності зв'язку, електронні довірчі послуги, місцеві державні адміністрації, місцеве самоврядування в Україні, громадські об'єднання, охоронну діяльність, інформацію, захист інформації в інформаційно-телекомунікаційних системах, доступ до публічної інформації тощо. До цього законодавчого блоку слід віднести й окремі положення Кодексу України про адміністративні правопорушення, Кримінального кодексу України та Кодексу цивільного захисту України.

3. Запропоновано привести приписи ст. 25 Закону України «Про критичну інфраструктуру» відповідно до положень Закону України «Про публічно-приватне партнерство». Крім того, у чинній редакції Закону України «Про критичну інфраструктуру» відсутні кореляційні положення щодо Закону України «Про концесію» в частині концесійного договору та інформації про об'єкти критичної інфраструктури.

4. Визначено напрями резильентності критичної інфраструктури міст України, що першочергово потребують правового врегулювання.

5. Впорядковано підзаконний блок законодавства, що безпосередньо пов'язаний із базовим законом про критичну інфраструктуру.

6. Обліковано частину нормативно-правових актів, які не згадуються в законі про критичну інфраструктуру, але регулюють відносини, тісно пов'язані із цією сферою.

7. Виокремлено базові цілі Національного плану захисту та забезпечення безпеки та стійкості в контексті правового забезпечення резильентності об'єктів критичної інфраструктури міст України.

8. Встановлено зв'язок між категоріями «відкритість міста» (управління, населення і середовище) та «захист критичної інфраструктури», який виявляється в тому, що відкритість забезпечує децентралізований моніторинг і швидке реагування за допомогою громади, а захищеність інфраструктури гарантує стабільне функціонування міського середовища та його комунікацій.



Декларації

Фінансування. Дослідження виконано без зовнішнього фінансування, у рамках науково-дослідної роботи Державної установи «Інститут економіко-правових досліджень імені В. К. Мамутова Національної академії наук України» «Економіко-правовий вимір резильєнтності міст України» (номер державної реєстрації 0125U000831)

Конфлікт інтересів. Автор заявляє про відсутність конфлікту інтересів.

Подяки. Автор висловлює подяку заступнику директора Інституту з наукової роботи Руслану Джабраїлову за консультації з окремих питань дослідження.

Використання штучного інтелекту. Інструменти штучного інтелекту під час підготовки статті не використовувалися.

Список використаних джерел

1. Про критичну інфраструктуру. Закон України від 16.11.2021 р. № 1882-IX. Верховна Рада України. Законодавство України. URL: <https://zakon.rada.gov.ua/laws/show/1882-20> (дата звернення: 09.07.2026).
2. Щодо Комплексних планів стійкості регіонів та окремих міст. Рішення Ради національної безпеки і оборони України від 03.03.2026 р., введено в дію Указом Президента України від 14.03.2026 р. № 239/2026. Верховна Рада України. Законодавство України. URL: <https://zakon.rada.gov.ua/laws/show/n0018525-26> (дата звернення: 09.07.2026).
3. Плахотнюк Р. В. Забезпечення стійкості критичної інфраструктури в Україні в умовах сучасних викликів. *Економічний простір*. 2024. № 195. С. 47–54. <https://doi.org/10.30838/EP.195.47-54>.
4. Ковальчук А. Т. Система правового регулювання захисту об'єктів критичної інфраструктури в Україні: сучасний стан та напрями удосконалення. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 90, ч. 5. С. 172–184. <https://doi.org/10.24144/2307-3322.2025.90.5.21>.
5. Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України. Аналіз. доп. Київ : НІСД, 2019. 224 с.
6. Богдан Б. В. Державна політика у сфері захисту критичної інфраструктури під час дії воєнного стану. *Юридичний науковий електронний журнал*. 2025. № 1, С. 828–830. <https://doi.org/10.32782/2524-0374/2025-1/199>.
7. Ковальов К. Є. Сучасні виклики та загрози для критичної інфраструктури України під час воєнного стану. *Приватне та публічне право*. 2025. № 1. С. 75–80. <https://doi.org/10.32782/2663-5666.2025.1.12>.
8. Aebi S., Hauri A., Kamberaj J. Critical Infrastructure Resilience in Ukraine: Energy, Transportation, and Communication. *Risk and Resilience Report*. <https://doi.org/10.3929/ethz-b-000662463>.
9. Irankunda G., Zhan W., Fernand M., Zhang J. Assessing the Resilience of Critical Infrastructure Facilities toward a Holistic and Theoretical Approach: A Multi-Scenario Evidence and Case Study. *Sustainability*. 2024. № 16. 8735. <https://doi.org/10.3390/su16208735>.
10. Wolbach M., Talukder R. The value of EU research projects in critical infrastructure protection. *Terrorism — Studies, Analyses, Prevention*. 2025. special edition. Pp. 315–339. <https://doi.org/10.4467/27204383TER.25.024.21527>.
11. Кірін Р. С. Правове забезпечення комплексної резильєнтності міст України. *Український політико-правовий дискурс*. 2025. № 13. DOI: [10.5281/zenodo.16657770](https://doi.org/10.5281/zenodo.16657770). URL: <https://ppdnz.com.ua/index.php/home/article/view/357>.
12. Кірін Р. С., Хоменко В. Л., Пашенко О. А. Інноваційна складова резильєнтності міста: цифрові та правові виміри. *Актуальні питання у сучасній науці. Серія:*



- Право*. 2025. № 7 (37), С. 447–468. [https://doi.org/10.52058/2786-6300-2025-7\(37\)-447-468](https://doi.org/10.52058/2786-6300-2025-7(37)-447-468).
13. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р. № 2163–VIII. *Верховна Рада України. Законодавство України*. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 09.07.2026).
 14. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості». Указ Президента України від 27.09.2021 р. № 479/2021. *Верховна Рада України. Законодавство України*. URL: <https://zakon.rada.gov.ua/laws/show/479/2021> (дата звернення: 09.07.2026).
 15. Кірін Р. С. Актуальні проблеми урбаністичного права: відкритість, цифровізація, резильєнтність. Київ, Дніпро : Журфонд, 2026. 610 с. <https://doi.org/10.35668/978-617-14-0514-1>.
 16. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури. Розпорядження Кабінету Міністрів України від 19.09.2023 р. № 825–р. *Верховна Рада України. Законодавство України*. URL: <https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80> (дата звернення: 09.07.2026).
 17. 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. OJ L 333, 27.12.2022, pp. 164–198. *EUR-Lex*. ELI: <http://data.europa.eu/eli/dir/2022/2557/oj> (дата звернення: 09.07.2026).
 18. 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). *EUR-Lex*. URL: <http://data.europa.eu/eli/dir/2022/2555/2022-12-27> (дата звернення: 09.07.2026).
 19. Council Recommendation of 25 June 2024 on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance. OJ C, C/2024/4371, 5.7.2024. *EUR-Lex*. ELI: <http://data.europa.eu/eli/C/2024/4371/oj> (дата звернення: 09.07.2026).
 20. Устименко В., Тарасевич О., Кірін Р., Панкова Л. Економіко-правове забезпечення відкритості міст України. *Економіка України*. 2025. Том 68, № 2 (759). С. 28–46. <https://doi.org/10.15407/economyukr.2025.02.028>.
 21. Про внесення змін до Закону України «Про місцеве самоврядування в Україні» щодо забезпечення прозорості місцевого самоврядування. Закон України від 22.02.2024 р. № 3590–IX. *Верховна Рада України. Законодавство України*. URL: <https://zakon.rada.gov.ua/laws/show/3590-20> (дата звернення: 09.07.2026).
 22. Про внесення змін до деяких законодавчих актів України щодо забезпечення законності та прозорості в діяльності органів місцевого самоврядування : Закон України від 05.11.2025 р. № 4677–IX. *Верховна Рада України. Законодавство України*. URL: <https://zakon.rada.gov.ua/laws/show/4677-20> (дата звернення: 09.07.2026).
 23. Кірін Р., Шеховцов В. «Відкрите місто»: поняття та правові засади. *Baltic Journal of Legal and Social Sciences*. 2022. № 2. С. 96–103. <https://doi.org/10.30525/2592-8813-2022-2-16>.



ENGLISH METADATA

Roman KIRIN

State Organization V. Mamutov Institute of Economic and Legal Research of NAS of Ukraine, Kyiv, Ukraine

Legal Framework for the Resilience of Critical Infrastructure in Ukrainian Cities

Abstract. This article examines current issues related to the legal framework for ensuring the resilience of critical infrastructure in Ukrainian cities. It argues that the specific nature of the formation and development of the legal framework governing critical infrastructure lies in the fact that the basic law regulates relations concerning the operation and protection of critical infrastructure as a whole and its facilities during peacetime. This reveals the cross-sectoral nature of the legal framework governing critical infrastructure, which contains provisions falling under various areas of Ukrainian law, including national security and defence, urban planning, transportation, telecommunications, local self-government, public associations, security activities, information, and more. It is proposed to bring the provisions of Article 25 of the Law of Ukraine “On Critical Infrastructure” into line with the provisions of the Law of Ukraine “On Public-Private Partnerships.” Furthermore, the current version of the framework law lacks provisions that align with the Law of Ukraine “On Concessions.” The areas of critical infrastructure resilience in Ukrainian cities that require priority legal regulation have been identified: the energy sector; water supply and wastewater management; healthcare; transportation and logistics; telecommunications and IT; resilience of local governments; civil protection; migration and demographic resilience; — resilience of city residents; financial and economic resilience. This document systematises the body of subordinate legislation directly related to the framework law on critical infrastructure, as well as certain regulatory acts that are not mentioned in the law on critical infrastructure but regulate relations in this area. The fundamental objectives in the context of ensuring the resilience of critical infrastructure facilities in Ukrainian cities are identified. A connection is established between the categories of “city openness” and “critical infrastructure protection,” which currently involve a delicate balance. The key aspects of the interaction between these concepts are: protection of critical technological information, information security, and cybersecurity; transparency in procurement and tenders; risk management and communication; citizen engagement.

Keywords: national security, compliance with legislation, local self-government, regulatory and legal acts, protection, stability.

Received: 17 July 2026. Accepted: 02 September 2026

Published online: 23 September 2026. Published in print: 30 October 2026

Для цитування / How to cite:

ДСТУ 8302:2015: Кірін Р. Правове забезпечення резильєнтності критичної інфраструктури міст України. *Університетські наукові записки*. 2026. № 5 (113). С. 103–114. DOI: <https://doi.org/10.37491/UNZ.113.6>.

APA 7th: Kirin, R. (2026). Legal Framework for the Resilience of Critical Infrastructure in Ukrainian Cities. *University Scientific Notes*, (5(113), 103–114. DOI: <https://doi.org/10.37491/UNZ.113.6>.