Ігор КОЗИЧ
ORCID: 0000-0002-8746-1154

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У ВИМІРІ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ

УДК 343.2.01

Директива 2008/114/ЄС від 8 грудня 2008 року [1] «Про ідентифікацію та призначення європейської критичної інфраструктури та оцінку необхідності поліпшення її захисту» фактично стала першим документом Європейського Союзу у відповідній сфері, проклавши шлях до наднаціональної інтеграції питань захисту критичної інфраструктури. Основна увага в Директиві 2008 року була зосереджена на концепції захисту (Critical Infrastructure Protection — CIP), що передбачала передусім ідентифікацію конкретних фізичних об'єктів та вжиття заходів для їх убезпечення від терористичних атак та інших навмисних загроз. Такий підхід базувався на традиційному управлінні ризиками з метою уникнення та запобігання небажаним подіям у визначених секторах.

Секторальне охоплення Директиви 2008 року було суттєво обмеженим, адже після тривалих дискусій було визнано лише два сектори — енергетику та транспорт (Додаток 1 Директиви). Для того, щоб об'єкт отримав статус європейської критичної інфраструктури (ЄКІ), його порушення або знищення мало б спричинити значний транскордонний вплив щонайменше на дві (стаття 2(b)) держави-члени ЄС.

Проте проведена у 2019 році оцінка функціонування Директиви 2008/114/ЄС виявила її інституційну обмеженість в умовах дедалі більшої взаємопов'язаності та транскордонного характеру операцій [3], оскільки було встановлено, що захисні заходи, спрямовані лише на окремі фізичні об'єкти, є недостатніми для запобігання всім можливим збоям у наданні послуг.

Сучасна трансформація європейського законодавства у сфері безпеки критичної інфраструктури, що ознаменувалася прийняттям Директиви (ЄС) 2022/2557 (далі - Директива CER[1] [3]),

1 CER - critical entities resilience

яка остаточно скасувала дію Директиви 2008/114/ЄС з 18 жовтня 2024 року, свідчить про фундаментальний парадигмальний зсув у підходах до забезпечення життєдіяльності суспільства: якщо попередня Директива 2008/114/ЕС фокусувалася переважно на захисті (protection) фізичної цілісності окремих об'єктів, то новий акт акцентує увагу на їх стійкості (resilience).

Стійкість у контексті Директиви CER визначається як здатність суб'єкта не лише запобігати інцидентам, а й ефективно реагувати, поглинати (пом'якшувати, нейтралізувати його наслідки) та відновлюватися після подій, що мають потенціал порушити надання життєво важливих послуг (стаття 2(2)) [3].

Для кримінально-правової політики України цей перехід ставить ряд серйозних викликів, в першу чергу щодо переосмислення об'єкта злочинного посягання. Очевидним є той факт, що у чинному кримінальному законодавстві норми, що забезпечують охорону критичної інфраструктури, розпорошені за різними розділами Особливої частини КК України, де основними об'єктами виступають національна безпека, власність, громадська безпека або безпека руху та експлуатації транспорту тощо. Однак концепція стійкості вимагає зміщення акценту на захист самого процесу надання послуг, що є критичними для підтримання життєво важливих суспільних функцій чи економічної діяльності на внутрішньому ринку. Таким чином, спрямуванням реформування кримінального законодавства з ціллю забезпечення такої стійкості (а відтак - формуванням запиту до кримінально-правової політики) стає не стільки «бетон і залізо» конкретної споруди, скільки функціональна спроможність системи витримувати зовнішні та внутрішні навантаження, включаючи наслідки зміни клімату, гібридні загрози чи воєнні дії (в контексті України).

Крім того, розширення секторальної охорони, передбачене Директивою CER, також вимагає суттєвої корекції кримінально-правового інструментарію. Якщо раніше європейське регулювання обмежувалося секторами енергетики та транспорту [1], то тепер перелік охоплює одинадцять критичних галузей, зокрема банківську сферу, охорону здоров'я, цифрову інфраструктуру, державне управління, космос та харчову промисловість тощо

(див. Додаток до Директиви CER). Таке розширення створює складну «систему систем», де взаємозалежність між секторами означає, що будь-який інцидент може мати подальші вторинні наслідки, виходячи далеко за межі однієї установи чи навіть держави.

Така концепція «каскадної шкоди» (cascading effects), що згадується у пункті (5) преамбули Директиви CER, додає ще один рівень складності до правової оцінки інцидентів, закладаючи її в основу вимог щодо оцінки ризиків у Статтях 7 та 12. Оскільки збій в одному секторі може спричинити «ефект доміно» в інших, кримінальна відповідальність повинна визначатися не лише за прямими збитками, а й за масштабом системної дестабілізації суспільства, що ставить питання про необхідність врахування системних ризиків та диференціації санкцій залежно від вторинних наслідків посягання на об'єкт, порушення функціонування якого може призвести до розвитку кризових ситуацій від місцевого до загальнодержавного рівня.

Якщо не вести мову про загальні норми, що забезпечують охорону в т.ч. об'єктів критичної інфраструктури (диверсія, тероризм і т.п.), то варто визнати, що українська кримінально-правова доктрина та законодавча практика направду зосереджена, приміром, на об'єктах енергетики (напр. ст. 194-1 КК [4]) чи транспортних комунікаціях (напр. ст. 279 КК [4]), що в цілому відповідає логіці старої Директиви 2008 року [1]. Проте імплементація підходу «стійкості» вимагає розширення правового поля на такі сфери, як банківська справа, охорона здоров'я, продовольча безпека та космос, які наразі не мають спеціалізованої кримінально-правової охорони саме як об'єкти критичної інфраструктури.

Зокрема, сектор охорони здоров'я, що охоплює не лише надання медичних послуг, а й дослідження, розробку та виробництво критично важливих лікарських засобів, вимагає перегляду диспозицій статей, які наразі захищають відповідний об'єкт лише в загальному сенсі, без контексту CER, хоча кримінально-правова політика при нормотворенні має враховувати, що, до прикладу, посягання на логістичні ланцюжки постачання медикаментів або на цілісність дослідницьких лабораторій у період воєнного стану

може розглядатися як посягання на стійкість об'єктів критичної інфраструктури загалом. Аналогічна ситуація спостерігається і в секторі виробництва та розподілу продуктів харчування: попри наявність відповідних статей, вони не враховують стратегічного значення великих логістичних центрів як елементів критичної інфраструктури, порушення роботи яких може призвести до системної гуманітарної кризи.

Аналогічно, окремої уваги потребує цифрова інфраструктура, де спостерігається найбільш виразне змішування фізичних та кібернетичних загроз (хоча кримінальне законодавство повинно забезпечувати захист не лише «кабелів», а й хмарних сервісів, центрів обробки даних та точок обміну інтернет-трафіком як критичних суб'єктів в контексті концепції CER); банківська справа та інфраструктура фінансового ринку тощо. Хоча ці сфери регулюються спеціальним законодавством, у вимірі CER вони стають частиною єдиної «системи систем», де збій у фінансових транзакціях може паралізувати інші сектори, наприклад, енергетику чи транспорт. Запитом до кримінально-правової політики у цьому контексті є, до прикладу, вирішення питання про можливість систематизації чи введення норм, які б кваліфікували посягання на критичні фінансові операційні системи як правопорушення проти безпеки критичної інфраструктури.

Важливим аспектом адаптації українського законодавства до вимог CER є вирішення проблеми термінологічної неузгодженості. У національному правовому полі спостерігається дисонанс між термінами «критично важливі об'єкти інфраструктури», що вживаються у Кримінальному кодексі [4], та дефініціями профільного Закону України «Про критичну інфраструктуру» [5]. А Директива CER взагалі запроваджує нову юридичну категорію — «критичний суб'єкт» (critical entity), що є ширшою за поняття фізичного об'єкта та охоплює оператора, відповідального за забезпечення стійкості. Окремі науковці вважають, що такий підхід, ймовірно, спрямований на плавний перехід від секторів критичної інтеграції (таких як енергетика) до більш конкретних операторів (таких як енергетична компанія) або, можливо, об'єкта (електростанції) для покращення та сприяння більш детальному моніторингу та регулюванню [6].

Також треба враховувати, що імплементація концептів нової Директиви CER, яка, як вже було зазначено, запроваджує категорію «критичний суб'єкт» (critical entity), вносить додатковий рівень складності в контексті нормотворчої функції кримінально-правової політики. Так, в європейському контексті це поняття є еквівалентним оператору критичної інфраструктури, і його введення має на меті змістити акцент із захисту статичних активів на динамічну діяльність організацій, що забезпечують життєво важливі сервіси. В українському законодавчому полі подібна термінологічна інновація може викликати плутанину, оскільки офіційні переклади терміну «entity» у різних мовних версіях Директиви CER варіюються від «установи» та «актора» до «відповідального суб'єкта», що створює ризики різних національних інтерпретацій. Для кримінально-правової політики України це означає необхідність не просто замінити одне слово іншим, а узгодити кримінально-правову лексику із управлінсько-адміністративно-правовими категоріями, що визначають відповідальність операторів за забезпечення стійкості.

Більше того, термінологічна неузгодженість проявляється і у відсутності в КК України концептуального апарату для опису «стійкості» (resilience) в контексті забезпечення кримінально-правової охорони. Якщо Директива CER визначає стійкість через здатність запобігати, реагувати, поглинати та відновлюватися після інцидентів, то вітчизняні кримінально-правові норми досі зосереджені на термінах «знищення», «пошкодження» або «руйнування», що фактично описують лише фізичний вплив відповідного рівня. Така вузька інтерпретація ігнорує сучасні виклики, коли стійкість об'єкта може бути підірвана без фізичного пошкодження — наприклад, через злочинне втручання в алгоритми управління чи логістичні процеси. Відтак, запитом до правотворця є впровадження в КК України відповідної термінології, яка б охоплювала, наприклад, «порушення належного функціонування» або «втрату стійкості».

Типологія небезпек, закладена у Статті 5 Директиви CER, вимагає від держав-членів проведення оцінки ризиків, що враховує не лише традиційні безпекові виклики, а й надзвичайні ситу-

ації у сфері охорони здоров'я, наслідки зміни клімату та складні гібридні загрози, новітні загрози у ході воєнних дій тощо. Тому запровадження ризик-орієнтованого підходу, що є ще одною відмітною рисою Директиви CER, формує якісно нові виклики для кримінально-правової політики, оскільки вимагає переходу від реагування на фактичне заподіяння шкоди до превентивного захисту потенційно вразливих вузлів системи. У межах цього підходу ризик визначається як потенціал для втрати або порушення роботи, що виражається через врахування масштабу наслідків та ймовірності виникнення інциденту. Для кримінально-правової політики це означає необхідність розробки доктринальних засад відповідальності не лише за пряме фізичне знищення, а й за створення умов, що підвищують вразливість критичних суб'єктів до загроз різного характеру.

До речі, впровадження підходу «всіх загроз» (all-hazards approach), що також становить концептуальне осердя Директиви CER, знаменує собою остаточний перехід від реагування на окремі загрози до формування універсальної рамки забезпечення стійкості. Якщо попередня Директива 2008/114/ЄС [1] була значною мірою зосереджена на протидії тероризму та захисті фізичної цілісності енергетичних і транспортних об'єктів, то нова правова конструкція 2022 року виходить із того, що природа загрози є вторинною щодо її наслідків для життєво важливих суспільних функцій. Згідно з пунктом (4) преамбули Директиви CER, такий підхід охоплює будь-які інциденти — від природних катаклізмів та техногенних аварій до навмисних антагоністичних дій, включаючи терористичні злочини та злочинне проникнення. Для кримінально-правової політики України це породжує новий запит щодо відмови від фрагментарної охорони окремих об'єктів власності на користь системного захисту «безперервності сервісів» у всіх визначених секторах.

Окрему увагу приділено внутрішнім загрозам, що актуалізує питання криміналізації зловживань правами доступу з боку персоналу. Директива CER підкреслює зростаюче занепокоєння щодо можливості зловживання правами доступу з боку персоналу або підрядників для нанесення шкоди критичним суб'єктам.

Це вимагає від кримінально-правової політики розробки механізмів відповідальності, які б корелювали із зобов'язаннями суб'єктів проводити ретельні перевірки персоналу (background checks), включаючи аналіз кримінального минулого (Преамбула (32)). Викликом тут є дотримання балансу між інтересами національної безпеки та захистом персональних даних, що потребує чіткої законодавчої регламентації умов, за яких невиконання таких перевірок може тягнути за собою кримінальну відповідальність службових осіб у разі настання тяжких наслідків.

Крім того, Статті 12 та 13 Директиви CER покладають на критичні суб'єкти обов'язок не лише проводити регулярну оцінку «всіх небезпек», а й вживати технічних та організаційних заходів для забезпечення стійкості. У вимірі кримінально-правової політики це формує запит на встановлення, до прикладу, відповідальності за грубе ігнорування стандартів безпеки, що призвело до втрати здатності об'єкта адаптуватися до інцидентів та відновлюватися після них.

Підсумовуючи, можна стверджувати, що трансформація кримінально-правової політики України у світлі Директиви CER має відбуватися через консолідацію норм, спрямованих на захист критичної інфраструктури, та впровадження механізмів, що враховують динамічний спектр всіх можливих загроз. Подальша побудова архітектури кримінально-правової охорони критичної інфраструктури повинна базуватися на розумінні стійкості як здатності відповідного елемента зберігати функціональність за будь-яких умов, що потребує чіткої диференціації відповідальності та гармонізації національних стандартів із європейськими вимогами щодо захисту критичних суб'єктів.

1. *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union. 2008. L 345. P. 75–82.*
2. *Evaluation study of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Final report. URL: https://www.sipotra.it/wp-content/uploads/2020/06/Evaluation-study-of-Council-Directive-*

2008114-on-the-identification-and-designation-of-European-critical-infrastructures-and-the-assessment-of-the-need-to-improve-thei.pdf

3. *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 . Official Journal of the European Union. 2022. L 333. P. 164–198.*
4. *Кримінальний кодекс України : Закон України від 05 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14*
5. *Про критичну інфраструктуру : Закон України від 16 листоп. 2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20.*
6. *Pursiainen C., Kytömaa E. From protecting European critical infrastructure to the resilience of European critical entities: what does it mean?. Sustainable and Resilient Infrastructure . 2023. Vol. 8, No. S1. P. 85–101. DOI: 10.1080/23789689.2022.2128562.*

Козич І. В. Забезпечення стійкості об'єктів критичної інфраструктури у вимірі кримінально-правової політики

Стаття присвячена комплексному аналізу трансформації національної кримінально-правової політики України в умовах адаптації до сучасних європейських стандартів безпеки критичної інфраструктури (КІ). Основна увага приділяється дослідженню фундаментального парадигмального зсуву, задекларованого у Директиві (ЄС) 2022/2557 (Директива CER), що полягає у переході від концепції «захисту» (protection) фізичних активів до забезпечення їхньої «стійкості» (resilience). Автор обґрунтовує, що для кримінально-правової доктрини цей перехід означає необхідність переосмислення об'єкта злочинного посягання: фокус охорони зміщується з матеріальної цілісності споруд («бетону і заліза») на функціональну спроможність системи безперебійно надавати життєво важливі послуги суспільству.

У роботі детально проаналізовано виклики, пов'язані із розширенням секторальної охорони з двох (енергетика та транспорт) до одинадцяти критичних галузей, що створює складну «систему систем» та актуалізує концепцію «каскадної шкоди» (cascading effects). Доведено, що кримінальна відповідальність у цій сфері повинна диференціюватися не лише за обсягом прямих збитків, а й за масштабом системної дестабілізації, яку спричиняє «ефект доміно» при посяганні на взаємопов'язані об'єкти. Окремий акцент зроблено на імплементації підходу «всіх небезпек» (all-hazards approach) та ризик-орієнтованого підходу, що вимагає від кримінально-правової політики переходу до превентивного захисту потенційно вразливих вузлів інфраструктури.

Значну увагу приділено проблемі термінологічної неузгодженості між чинним Кримінальним кодексом України та профільним законодавством, зокрема щодо дефініцій «критично важливий об'єкт» та «критичний суб'єкт».

Наголошується, що ефективна кримінально-правова політика має базуватися на консолідації норм та гармонізації національних стандартів із вимогами

CER для забезпечення національної безпеки в умовах динамічних гібридних загроз та воєнних дій.

Ключові слова: кримінально-правова політика, об'єкт кримінально-правової охорони, імплементація законодавства ЄС, критична інфраструктура, криміналізація, злочини проти основ національної безпеки, кримінальні правопорушення проти громадської безпека, кримінальні правопорушення в сфері енергетики, кримінальні правопорушення проти власності, кримінальні правопорушення проти здоров'я населення, кримінальні правопорушення проти безпеки руху та експлуатації транспорту.

Kozych I. V. Ensuring the resilience of critical infrastructure facilities in the dimension of criminal law policy

The article is devoted to a comprehensive analysis of the transformation of the national criminal law policy of Ukraine in the context of adaptation to modern European standards of critical infrastructure (CI) security. The main attention is paid to the study of the fundamental paradigm shift declared in Directive (EU) 2022/2557 (CER Directive), which consists in the transition from the concept of «protection» of physical assets to ensuring their «resilience». The author argues that for criminal law doctrine this transition means the need to rethink the object of criminal encroachment: the focus of protection shifts from the material integrity of structures («concrete and iron») to the functional ability of the system to continuously provide vital services to society.

The paper analyzes in detail the challenges associated with the expansion of sectoral protection from two (energy and transport) to eleven critical industries, which creates a complex "system of systems" and actualizes the concept of "cascading effects". It is proven that criminal liability in this area should be differentiated not only by the amount of direct damage, but also by the scale of systemic destabilization caused by the "domino effect" when attacking interconnected objects. Special emphasis is placed on the implementation of the "all-hazards approach" and the risk-oriented approach, which requires criminal law policy to transition to preventive protection of potentially vulnerable infrastructure nodes.

Considerable attention is paid to the problem of terminological inconsistency between the current Criminal Code of Ukraine and relevant legislation, in particular regarding the definitions of "critically important object" and "critical subject".

It is emphasized that effective criminal law policy should be based on the consolidation of norms and harmonization of national standards with the requirements of the CER to ensure national security in the context of dynamic hybrid threats and military operations.

Keywords: criminal law policy, object of criminal law protection, implementation of EU legislation, critical infrastructure, criminalization, crimes against the foundations of national security, criminal offenses against public safety, criminal offenses in the energy sector, criminal offenses against property, criminal offenses against public health, criminal offenses against traffic safety and transport operation.