УДК 351.746.1:343.3:007.51(477)
DOI https://doi.org/10.24144/2788-6018.2025.04.3.22

ГЕНЕЗА ПОНЯТТЯ «КРИТИЧНА ІНФРАСТРУКТУРА» У КОНТЕКСТІ ПРОТИДІЇ СЛУЖБОЮ БЕЗПЕКИ УКРАЇНИ ЗАГРОЗАМ НА ЇЇ ОБ'ЄКТАХ

Герасименко О.М.,
кандидат юридичних наук, докторант,
Національна академія Служби безпеки України
ORCID: 0009-0005-5078-3829

Герасименко О.М. Генеза поняття «критична інфраструктура» у контексті протидії Службою безпеки України загрозам на її об'єктах.

Стаття присвячена аналізу генези поняття «критична інфраструктура» в українському правовому полі та визначенню ролі протидії СБУ кримінальним правопорушенням на її об'єктах у системі забезпечення національної безпеки. У контексті гібридної війни, кіберзагроз і зростаючої вразливості систем життєзабезпечення України поняття терміну «критична інфраструктура» набуло вагомого юридичного та кримінологічного значення. У статті досліджено еволюцію терміну від його початкового використання у військовій термінології до сучасного розуміння як комплексу фізичних і віртуальних систем, що забезпечують стабільність функціонування держави, суспільства та економіки.

На основі аналізу міжнародного досвіду, зокрема законодавства США та Європейського Союзу, простежено становлення концепції критичної інфраструктури, починаючи з 1980-х років, коли в США було визначено її як сукупність взаємопов'язаних елементів, що підтримують суспільну структуру, до сучасних європейських підходів, які акцентують увагу на мультисекторальності та запобіганні каскадним ефектам. В Україні формування поняття почалося пізніше, його формування зумовлене історичними особливостями пострадянського розвитку та сучасними викликами та загрозами. Ключовими етапами стали видання «Зеленої книги» (2015) та прийняття Закону України «Про критичну інфраструктуру» (2021), які імплементували ризик-орієнтований підхід до визначення та захисту критичної інфраструктури.

Особлива увага приділена кримінально-правовим аспектам захисту об'єктів критичної інфраструктури. У статті проаналізовано сучасні загрози, зокрема тероризм, диверсії та кібератаки, які становлять екзистенційну небезпеку для національної безпеки України. Запропоновано класифікацію злочинів проти критичної інфраструктури за критеріями спрямованості, технологічного вектора та ступеня каскадності наслідків. Акцентовано увагу на необхідності вдосконалення тактики забезпечення розслідувань, зокрема шляхом застосування цифрової форензики, вибухотехнічної експертизи та міжнародного співробітництва. Визначено прогалини у чинному законодавстві, зокрема відсутність спеціальних норм для кримінальної відповідальності за посягання на об'єкти критичної інфраструктури, та запропоновано низку заходів для їх усунення, включаючи кодифікацію методик категоризації об'єктів, створення спеціалізованих груп процесуального керівництва та вдосконалення підготовки кадрів.

Підкреслено, що генеза поняття «критична інфраструктура» в Україні відображає перехід від економічного до комплексного кримінально-правового розуміння. Запропоновано інтегрований ризик-орієнтований підхід, який поєднує системно-функціональну та секторно-категоріальну класифікацію для ефективного захисту критичної інфраструктури та протидії злочинним посяганням.

Ключові слова: критична інфраструктура, національна безпека, кримінальні правопорушення, кіберзагрози, тероризм, криміналістичне забезпечення, ризик-орієнтований підхід.

Herasymenko O.M. Genesis of the concept of "critical infrastructure" in the context of the security service of ukraine's counteraction to threats at its facilities.

The article is devoted to the analysis of the genesis of the concept of «critical infrastructure» in the Ukrainian legal field and the definition of the role of the SBU in countering criminal offenses at its facilities in the system of ensuring national security. In the context of hybrid warfare, cyber threats and the growing vulnerability of Ukraine's life support systems, the concept of the term "critical infrastructure" has acquired significant legal and criminological significance. The article examines the evolution of the term from its initial use in military terminology to its modern understanding as a complex of physical and virtual systems that ensure the stable functioning of the state, society and economy.

Based on the analysis of international experience, in particular the legislation of the USA and the European Union, the formation of the concept of critical infrastructure is traced, starting from the 1980s, when in the USA it was defined as a set of interconnected elements that support the social structure, to modern European approaches that emphasize multisectorality and the prevention of cascading effects. In Ukraine, the formation of the concept began later, its formation is due to the historical features of post-Soviet development and modern challenges and threats. The key stages were the publication of the "Green Book" (2015) and the adoption of the Law of Ukraine "On Critical Infrastructure" (2021), which implemented a risk-oriented approach to the definition and protection of critical infrastructure.

Particular attention is paid to the criminal law aspects of protecting critical infrastructure facilities. The article analyzes modern threats, in particular terrorism, sabotage and cyberattacks, which pose an existential threat to the national security of Ukraine. A classification of crimes against critical infrastructure is proposed according to the criteria of focus, technological vector and degree of cascading consequences. Attention is focused on the need to improve the tactics of ensuring investigations, in particular through the use of digital forensics, explosives examination and international cooperation. Gaps in the current legislation are identified, in particular the lack of special norms for criminal liability for encroachment on critical infrastructure facilities, and a number of measures are proposed to eliminate them, including the codification of methods for categorizing facilities, the creation of specialized procedural management groups, and the improvement of personnel training. It is emphasized that the genesis of the concept of «critical infrastructure» in Ukraine reflects the transition from an economic to a comprehensive criminal-legal understanding. An integrated risk-oriented approach is proposed, which combines system-functional and sector-categorical classification for effective protection of critical infrastructure and counteraction to criminal encroachment.

Key words: critical infrastructure, national security, criminal offenses, cyber threats, terrorism, forensic support, risk-oriented approach.

Постановка проблеми. Україна вступила у третє десятиліття XXI століття в умовах впливу реальних загроз національній безпеці і зростаючої вразливості ключових елементів систем життєзабезпечення. За цих обставин поняття «критична інфраструктура» вийшло за межі техніко-економічного дискурсу й набуло вагомого юридичного і кримінологічного змісту як індикатор загроз національній безпеці. У зв'язку з цим постає необхідність глибокого осмислення генези цього поняття в українському правовому полі та аналізу місця протидії СБУ кримінальним посяганням на її об'єкти, як складової державної політики.

Стан опрацювання проблематики. Проблематиці визначення поняття «критична інфраструктура», формування національної системи її захисту присвячено чимало наукових досліджень. Зокрема, Л. Арсенович дослідив інструментарій підвищення цифрової компетентності фахівців у сфері публічного управління захистом критичної інфраструктури (2024 р.) [1]; М. Бажанов ще в кінці 1990-х років окреслив загрози тероризму та інші виклики безпеці, що можуть впливати на стратегічно важливі об'єкти (1998 р.) [2]. Авторський внесок зробив О.В. Батюк, який у своїй монографії проаналізував криміналістичне забезпечення протидії злочинам на об'єктах критичної інфраструктури (2021 р.) [3]. Системне уявлення про кадрове забезпечення у цій сфері подано у роботі С. Бєлая, І. Євтушенка та В. Мацюка (2021 р.) [4], тоді як О. Васильєв звернув увагу на інфраструктурну підтримку регіонального розвитку в умовах загальнонаціональної безпеки (2007 р.) [5]. Проблемам кіберзагроз і кіберзахисту критичної інфраструктури присвячено низку праць, серед яких – дослідження М. Делембовського, В. Ткаченка і Д. Мельника (2024 р.) [6], О. Довганя та І. Чернухіна (2012 р.) [7], а також публікації, що висвітлюють кримінально-правові аспекти розслідування правопорушень проти критичних об'єктів – зокрема праця І. Єфіменка, В. Сліпченка та А. Вашка (2023 р.) [8] та огляд науково-практичних підходів у статті С. Кучерини і Д. Олєйнікова (2021 р.) [14]. Окрему увагу приділено нормативно-правовому забезпеченню функціонування та захисту критичної інфраструктури, зокрема у працях М. Коваліва з колективом (2021 р.) [10], М. Коваля та ін. (2023 р.) [11], Я. Курбанова (2016 р.) [13] і С. Ліпкана (2001 р.) [16]. Системні проблеми адміністративно-правового регулювання проаналізував С. Теленик (2021 р.) [21], а феномен кібератак в умовах війни – К. Черевко і Д. Пашнєв (2024 р.) [23].

Однак попри наявність численних наукових досліджень, присвячених формуванню системи захисту критичної інфраструктури в Україні, питання генези самого поняття «критична інфраструктура», а також визначення місця протидії СБУ кримінальним правопорушенням на відповідних об'єктах у національній системі їх захисту від загроз та у забезпечені національної безпеки України, на теоретико-правовому рівні залишаються недостатньо розробленими.

Метою дослідження є з'ясування особливостей становлення та розвитку поняття «критична інфраструктура» в українському правовому полі, а також визначення ролі та значення протидії

СБУ кримінальним правопорушенням на її об'єктах у національній системі їх захисту від загроз та у забезпечені національної безпеки України.

Виклад основного матеріалу. Поняття «критична інфраструктура», як засвідчує історико-науковий аналіз, зазнало суттєвої еволюції – від вузького розуміння комплексу тилових споруд у військовій термінології до надзвичайно широкого багаторівневого конструкта, що охоплює комплекс матеріальних і віртуальних систем, від яких залежить стабільність функціонування держави, суспільства, економіки та інших життєво важливих сфер. Перші концепції критичної інфраструктури (далі – КІ) у світовому дослідницькому обігу з'явилися у середині XX ст., а розширене трактування цього терміну сформувалося в економічній літературі як сукупність галузей, що забезпечують базові потреби суспільного відтворення.

Так, термін «інфраструктура» походить від латинських слів «infra» (нижче, під) та «structura» (будівля, розташування) і спочатку використовувався у військовому контексті для позначення тилових споруд, що забезпечували діяльність збройних сил [18, с. 269, 580]. У 1940–1950-х роках це поняття поступово перейшло в економічну сферу, охоплюючи широкий спектр галузей, таких як транспорт, енергетика, зв'язок, водопостачання тощо. У США вперше на національному рівні про критичну інфраструктуру заговорили у 1980-х роках, коли Національна дослідницька рада визначила її як сукупність взаємопов'язаних елементів, що підтримують цілісність суспільної структури, включаючи автомагістралі, мости, аеропорти, системи водопостачання та телекомунікації [32]. Остаточне формування концепції відбулося у 1996 році, коли в американському законодавстві було закріплено розуміння критичної інфраструктури як фізичних і віртуальних систем, порушення яких може мати катастрофічні наслідки для національної безпеки, економіки та здоров'я населення.

Ще наприкінці XX ст. було окреслено поняття «critical infrastructure» у зв'язку з посиленням терористичних, техногенних і природних загроз, яке тлумачилось як система фізичних чи віртуальних об'єктів, порушення функціонування яких може призвести до згубних наслідків для оборони, економіки, безпеки та здоров'я нації [34]. Ця ідея була покладена в основу формування американської політики захисту критичної інфраструктури, що передбачала, зокрема, прийняття відповідних актів – зокрема, Critical Infrastructure Information Act (2002) [27], створення окремих агентств у структурі Department of Homeland Security, розвиток міжсекторальної взаємодії та інформаційного обміну.

Значного розвитку це поняття набуло в дослідженнях Р. Нурксе, П Розенштейна-Родана, А. Хіршмана та ін., які розглядали інфраструктуру як ланку, що обслуговує економіку, що створює умови для стабільного функціонування виробничих систем [29; 30; 31].

У Європейському Союзі поняття почало активно вживатися наприкінці 1990-х років, зокрема у Великобританії, де акцент робився на захисті телекомунікацій, фінансового сектору та енергетики, а з 2004 року було започатковано Європейську програму захисту критичної інфраструктури (EPCIP), яка визначила її як об'єкти, системи та послуги, життєво важливі для суспільства [28], а також Директиву 2008/114/ЄС, де закріплено процедури ідентифікації та критерії «суттєвого впливу» для віднесення об'єктів до статусу європейської критичної інфраструктури. Директива Ради 2008/114/ЄС визначає критичну інфраструктуру як об'єкти, системи чи їх частини, функціонування яких має вирішальне значення для підтримання життєво важливих суспільних функцій, безпеки, добробуту населення [26]. В європейському дискурсі особлива увага приділяється мультисекторальності, міждержавному співробітництву, взаємозалежності ОКІ та запобіганню каскадних (доміно-) ефектів у разі їх ураження.

Таким чином, міжнародний досвід демонструє, що критична інфраструктура наразі розглядається як основа функціонування держави, а її захист та забезпечення безпеки є пріоритетом національної політики.

В Україні формування поняття «критична інфраструктура» відбувалося значно пізніше, що зумовлено як історичними особливостями розвитку держави, так і сучасними викликами. Як зазначається в наукових працях, питання захисту ключових ОКІ постало ще на початку 1990-х років, однак системний підхід до цього почав формуватися лише у 2010-х роках [13].

Українські дослідники пропонують трактувати критичну інфраструктуру як упорядковану єдність функціональних елементів і відносин, здатних забезпечити безперервне функціонування соціально-економічної системи та розвиток суспільства [24]. Як бачимо, сучасний науковий дискурс дедалі частіше акцентує увагу на необхідності системного підходу до інфраструктури, підкреслюючи її взаємозалежність, багатовекторність і вплив на всі основні сфери життєдіяльності держави.

Важливим кроком стало видання у 2015 році «Зеленої книги з питань захисту критичної інфраструктури в Україні», підготовленої Національним інститутом стратегічних досліджень, де було систематизовано наукові підходи до визначення цього поняття як систем і ресурсів, порушення яких призводить до серйозних негативних наслідків для суспільства та національної безпеки. Положен-

ня зазначеної книги містить формулювання КІ як «системи й ресурси, порушення функціонування яких спричиняє найсерйозніші негативні наслідки для життєдіяльності суспільства та національної безпеки» [9]. Українське законодавство, імплементуючи європейський ризик-орієнтований підхід, обрало широку, секторальну типологію: від енергетики й транспорту до фінансів, інформаційних мереж та охорони здоров'я. Вона охоплює, зокрема, електро- та газотранспортні системи, атомну енергетику, мережі зв'язку, системи е-урядування, а також масштабні харчові й агропромислові ланцюги. Водночас акцент робиться не лише на фізичному, а й на інформаційному та кіберпросторовому вимірах, що відображає зростання частки кіберзлочинів, спрямованих проти автоматизованих систем керування виробництвом та інфраструктурою.

Подальший нормативний розвиток відбувався через включення категорії КІ до Стратегії національної безпеки (2015) [22], а кульмінацією став Закон України «Про критичну інфраструктуру» 2021 р., що визначив КІ як «системи та ресурси, фізичні чи віртуальні, порушення яких спричиняє найсерйозніші наслідки для життєдіяльності суспільства та національної безпеки» [19]. Законотворець імплементував європейську формулу ризик-орієнтованого підходу, проте залишився на етапі загальних декларацій щодо кримінально-правової охорони її об'єктів відповідними суб'єктами.

Таким чином метою державної політики у сфері захисту від загроз критичної інфраструктури є забезпечення безпеки ОКІ, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури. До завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури належать запобігання проявам несанкціонованого втручання в її функціонування, прогнозування та попередження кризових ситуацій на об'єктах критичної інфраструктури, що порушують безпеку КІ.

Варто відзначити, що провідні українські дослідники пропонують різні концептуальні ракурси генези КІ. О. В. Васильєв трактує її передусім як «систему функціональних елементів і відносин», покликаних реалізувати інтереси групи економічних суб'єктів; його дефініція підкреслює процесуальний, динамічний характер інфраструктури та акцентує роль взаємодії «суб'єкт – об'єкт» у соціо-економічній системі [5, с. 23]. І. І. Чуницька, розширюючи цей підхід, вводить ознаку «органічної упорядкованої єдності», наголошуючи, що інфраструктура здатна не лише обслуговувати, а й «включатися» у суспільний розвиток, продукуючи нову соціальну якість[24, с. 252]. Натомість О.Д. Довгань і І.О. Чернухін пропонують ієрархічно-родову класифікацію об'єктів КІ: від технологічно керованих енергетичних та промислових вузлів до інформаційних систем Збройних сил; автори підкреслюють потребу диференційованого режиму охорони, але залишають відкритим питання критеріїв «небезпеки наслідків» у кожній категорії [7, с. 29, 31].

Тобто дискусія між цими підходами точиться навколо двох осей: (1) «структура – функція – ризик» і (2) «конститутивний елемент – нормативний статус». Системно-функціональний підхід (Васильєв – Чуницька) має перевагу інтегрального бачення й дозволяє врахувати міжсекторальні зв'язки, що критично важливо з погляду каскадних ефектів. Однак він ризикує залишити поза увагою формально-правові критерії віднесення об'єкта до КІ, що ускладнює правозастосування. Натомість родово-класифікаційна модель (Довгань – Чернухін) зручна для організації державного реєстру КІ та встановлення режимів охорони, але потребує гнучкого механізму періодичного перегляду категорій – інакше класифікація консервативно відстає від технологічної еволюції. Базована на директиві ЄС система оцінювання «масштаб + тяжкість наслідків» (географічне охоплення, демографічні та економічні збитки, екологічний і політичний ефект, тривалість шоку) пропонує третю вісь для синтезу: вона поєднує ризик-орієнтовану матрицю з нормативною визначеністю критеріїв.

На наш погляд, зважаючи на сучасні загрози, найбільш перспективним видається саме інтегрований ризик-орієнтований підхід, що комбінує мережеву, системно-функціональну оптику з юридичною чіткістю секторно-категоріальної класифікації.

Кримінально-правова площина проблеми формує другий тематичний пласт генези концепції КІ: від усвідомлення соціальної цінності об'єкта до криміналізації зазіхань на нього. У вітчизняному законодавстві базовим каркасом виступають ст.ст. 113, 194, 258, 277, 278, 279, 292, 361–363 КК України, які охоплюють терористичні акти, диверсії, руйнування шляхів сполучення та об'єктів енергетики, атаки на транспорт і засоби зв'язку. Науковий дискурс вирізняє щонайменше три позиції. Перша (В.А. Ліпкан) говорить про «злочини з елементами тероризму» як широку групу, що включає не лише прямі теракти, а й підготовку, фінансування, створення умов для них [16, с. 9]. Друга (А.М. Лисенко) пропонує легальний перелік статей КК, де терористична мета стає кваліфікуючою ознакою; цей підхід забезпечує ясність, але частково ігнорує змінювану природу загроз [15]. Третя, критична позиція (М.І. Бажанов) відхиляє термін «злочини терористичної спрямованості» як надто розмитий і застерігає від штучного розширення складу, відстоюючи принцип легальності та передбачуваності кримінального закону [2]. Найбільш продуктивним видається компромісний

варіант: ядром має залишатися чіткий перелік злочинів проти КІ, однак їх зміст слід коригувати через бланкетні відсилання до актуального переліку секторів КІ, сформований урядом.

Зазначене вище утворює науково-правову рамку, в межах якої Служба безпеки України (далі – СБУ) відіграє ключову роль у протидії загрозам на об'єктах КІ. Слід відзначити, що СБУ має ексклюзивні повноваження щодо протидії терористичним актам, кіберзагрозам, диверсіям та іншим протиправним діям. У практичній площині СБУ реалізує моделі протидії кримінальним правопорушенням, в яких використовуються взаємопов'язані компоненти: об'єкт, обстановка, порушник. Це дає можливість побудувати систему протидії СБУ кримінальним посяганням на ОКІ. Науковий аналіз функцій СБУ підтверджує, що остання спроможна активно запобігати, виявляти, припиняти і здійснювати досудове розслідування кримінальних посягань на об'єкти критичної інфраструктури, використовуючи інструментарій контррозвідувальної та оперативно-розшукової діяльності, превентивного кримінально-правового реагування, проведення спецоперацій і взаємодію з іншими державними інститутами та інше. Наприклад, поширеними є випадки коли під час досудового розслідування необхідно встановлювати цілий комплекс фактичних даних, що виходять за межі традиційного кола обставин. До них належать: масштабність наслідків, зокрема географічне охоплення території; наявність взаємозв'язку між пошкодженим елементом КІ та іншими системами (для виявлення каскадних ефектів); тривалість шкідливого впливу; ступінь вразливості об'єкта; тяжкість наслідків для економічної безпеки, життя і здоров'я населення, екології, обороноздатності та політичної стабільності [3, с. 41]. Розуміння місця та значення об'єкта в загальній системі КІ дозволяє встановити справжній умисел злочинців, який може бути спрямований не на сам об'єкт, а на спричинення більш віддалених та масштабних наслідків. Розслідування злочинів на ОКІ, особливо пов'язаних з кібератаками, неможливе без залучення спеціалістів у галузі інформаційних технологій, інженерії, енергетики тощо. Складність виявлення та фіксації цифрових слідів, необхідність аналізу складних технологічних процесів, а також транскордонний характер багатьох злочинів вимагають розвитку міжнародного співробітництва та вдосконалення механізмів надання правової допомоги.

Таким чином, протидія кримінальним правопорушенням на ОКІ – це синергія зусиль законодавця, що створює адекватну правову базу, правоохоронних органів, що здійснюють оперативно-слідчу діяльність, та науковців-криміналістів, які розробляють методики розслідування цих складних злочинів [8].

Наразі посягання на об'єкт критичної інфраструктури, яке вчиняється у кіберпросторі шляхом втручання в інформаційну інфраструктуру, розглядається як сукупність злочинів, хоча, і це цілком очевидно, вони співвідносяться як суспільно небезпечне діяння та спосіб його вчинення [14]. Це вказує на спорадичність кримінально-правової охорони об'єктів критичної інфраструктури та може призвести до формування неоднорідної слідчо-судової практики з цих питань.

Ефективна кримінально-правова протидія неможлива без чіткого розуміння та класифікації загроз, на які вона має реагувати. Законодавство України передбачає кваліфікацію злочинних посягань на об'єкти критичної інфраструктури за різними статтями КК України. Зокрема, це стосується статті 113 (Диверсія), статті 258 (Терористичний акт), статей 361-363 (Кіберзлочини), статті 194 (Умисне знищення майна) тощо [12].

Загрози КІ є різноманітними за своєю природою та джерелами походження. У нормативних документах ЄС та наукових працях їх зазвичай поділяють на кілька основних груп: природні небезпеки, техногенні аварії та зловмисні дії. Остання група, що включає тероризм, диверсії, злочинну діяльність та кібератаки має пряме відношення до сфери кримінального права. В умовах воєнного стану саме зловмисні дії становлять екзистенційну загрозу для національної КІ [33] та національної безпеки України.

Особливу небезпеку становить тероризм та злочини терористичної спрямованості. Об'єкти КІ, такі як атомні електростанції, греблі ГЕС, великі транспортні вузли чи хімічні підприємства, є привабливими цілями для терористів, оскільки атака на них може спричинити каскадні ефекти та масові жертви. У науковому середовищі триває дискусія щодо доцільності вживання терміну «злочини терористичної спрямованості». Деякі вчені, зокрема М.І. Бажанов, вважали його занадто розмитим для кримінального права [2]. Однак міжнародно-правові акти, ратифіковані Україною, зокрема Конвенція Ради Європи про запобігання тероризму, оперують поняттям «терористичний злочин», що легітимізує такий підхід [17]. Важливо, що Рада Безпеки ООН за ініціативи України ухвалила Резолюцію 2341 (2017), яка закликає держави забезпечити кримінальну відповідальність за терористичні атаки на об'єкти КІ [20].

Надзвичайно актуальною загрозою є кібератаки. Повсюдна цифровізація та впровадження автоматизованих систем управління технологічними процесами (АСУ ТП) на ОКІ робить їх вразливими до зламів. Кібератаки можуть бути спрямовані на виведення з ладу енергетичних систем, пору-

шення роботи транспорту, фінансових установ, державних реєстрів [10]. Ця загроза посилюється тим, що кібератаки можуть здійснюватися дистанційно, транскордонно та мати за мету не лише завдання прямої шкоди, але й ведення інформаційної війни та промислового шпигунства. Відсутність єдиної міжнародної термінології щодо понять «кіберпростір» та «кібербезпека» ускладнює вироблення спільних механізмів протидії.

Не можна ігнорувати й загрози фізичного впливу, як зовнішнього (підпали, вибухи, обстріли), так і внутрішнього, коли зловмисником виступає працівник об'єкта, що умисно порушує технологічні процеси. Окремо варто виділити біологічні загрози, актуальність яких продемонструвала пандемія COVID-19. Навмисне поширення небезпечних патогенів може паралізувати роботу ключових секторів економіки та суспільного життя. Усі ці зловмисні дії, що посягають на безпеку КІ, вимагають адекватної криміналізації та ефективних механізмів розслідування. Розуміння специфіки кожної загрози дозволяє слідчим та прокурорам правильно визначати обставини злочину, висувати обґрунтовані версії та обирати належні криміналістичні засоби для збору доказів.

Таким чином саме кримінальне право займає спеціальне місце в системі захисту критичної інфраструктури, що передбачає відповідальність за злочини проти держави, тероризм, диверсії, умисне знищення чи пошкодження об'єктів критичної інфраструктури. Дослідники С.Є. Кучерина та Д.О. Олєйніков у своєму науковому аналізі сучасного стану норм кримінального права, які встановлюють кримінальну відповідальність за посягання на об'єкти критичної інфраструктури, аргументовано довели, що чинний рівень кримінально-правової охорони об'єктів критичної інфраструктури є недостатнім та безсистемним [14]. Це зумовлено тим, що чинне кримінальне законодавство не передбачає індивідуалізованого підходу до критичної інфраструктури загалом і її об'єктів зокрема, а також не відображає сучасного стану розвитку організаційно-правових основ функціонування критичної інфраструктури. Крім того, кримінальний процес не містить індивідуалізованої тактики та підходів досудового розслідування кримінальних посягань на об'єкти критичної інфраструктури України, що на нашу думку впливає на ефективність з протидії СБУ кримінальним посяганням на ОКІ. Отже в системі протидії СБУ кримінальним правопорушенням на ОКІ існує ряд недоліків, які потребують системного опрацювання та вирішення науковим шляхом.

Так, кримінальні правопорушення проти КІ поділяються на дві великі групи: посягання з використанням засобів кібернетичного впливу та злочини фізичного характеру, зокрема диверсії, терористичні акти, крадіжки обладнання чи матеріалів [23]. Укладаючи криміналістичну типологію, пропонуємо систематизувати такі правопорушення за трьома критеріями: спрямованість (державна, публічна, приватна КІ), технологічний вектор атаки та ступінь каскадності наслідків.

Наразі традиційні інструменти кримінального права доповнюються спеціальними режимами. Зокрема, у ст. 113 КК України посилено відповідальність за диверсію, якщо її об'єктом є КІ; новелою 2024 р. у ст. 361-2 конкретизовано кваліфікуючі ознаки несанкціонованого втручання в інформаційні системи об'єктів КІ, що відображає імплементацію положень Будапештської конвенції про кіберзлочинність [12]. Одночасно адміністративні санкції у сфері техногенної безпеки використовуються як запобіжник проти недбалості операторів та постачальників послуг [21]. Однак ця діяльність є недостатньою для організації ефективної протидії СБУ кримінальним правопорушенням на ОКІ і потребує подальшого опрацювання.

Криміналістичне забезпечення превентивної діяльності полягає у необхідності розроблення методик виявлення і усунення умов, що сприяють скоєнню злочинів, а також у створенні реєстру криміногенних ризик-факторів специфічних для кожного сектору КІ. У вузькоінженерному аспекті системи відеоаналітики на базі штучного інтелекту дозволяють зменшити час реагування на вторгнення до енергетичних об'єктів, а використання LIDAR-моніторингу забезпечує об'єктивне документування обстрілів інфраструктури [25].

Спеціальне місце повинно відводиться процедурі огляду місця події на об'єктах КІ. Практика воєнного часу вимагає залучення інженерно-технічних підрозділів ЗСУ для первинного розмінування, після чого слідчо-оперативна група здійснює фіксацію пошкоджень програмно-апаратними комплексами тривимірного сканування [11]. Доказова база формується з урахуванням принципу неперервності життєвого циклу цифрових слідів, що передбачає їхню бекапізацію в хмарних репозитаріях із подвійним шифруванням [10].

Підвищення ефективності протидії неможливе без фахових кадрів. Вітчизняні дослідження підтверджують брак комплексної освітньої програми з безпеки КІ; усе ще превалює фрагментарна підготовка ІТ-спеціалістів та силовиків [4]. За пропозиціями експертної групи при МВС, освітня траєкторія має включати модулі криміналістичного забезпечення кіберрозслідувань, інженерного захисту об'єктів та crisis-management, що гарантуватиме міждисциплінарний характер підготовки [1].

У доктрині закордонного права превалює підхід про невіддільність кримінально-правового режиму КІ від концепції національної стійкості. Українська практика дедалі ширше застосовує прин-

ципproportionality of harm, коли тяжкість покарання корелює зі ступенем порушення безперервності послуг [33]. Так, за навмисне виведення з ладу вузлової підстанції електромережі, що спричинило масове відключення, суди кваліфікують дії за сукупністю ст. 258 та 361-4 КК із кумуляцією санкцій.

«Ефективна кримінально-правова охорона об'єктів критичної інфраструктури неможлива без синхронізації технологічних бар'єрів та процесуальних інструментів фіксації та аналізу доказів, інакше будь-яка вразливість мережі перетворюється на правову лакуну» [6].

Таким чином, державна політика у сфері захисту критичної інфраструктури, зокрема в частині протидії СБУ кримінальним правопорушенням на ОКІ, має базуватися на синтезі наукових підходів, ризик-орієнтаційної моделі, технічного моніторингу, кримінально-правової протидії, що дозволяє гарантувати запобігання, виявлення, припинення та досудове розслідування кримінальних посягань на ОКІ, безперервність функціонування критичних систем, зниження рівня загрози для життєдіяльності суспільства, що в цілому забезпечить сприятливий для розвитку держави рівень національної безпеки.

Висновки. Генеза поняття «критична інфраструктура» (КІ) демонструє трансформацію від економічного терміну до комплексної правової категорії, що є ключовою для національної безпеки. Формування концепції КІ в Україні прискорилося у 2010-х роках під впливом загроз. «Зелена книга» (2015) та Закон «Про критичну інфраструктуру» (2021) закріпили ризик-орієнтований підхід, визначивши КІ як систему об'єктів, порушення яких загрожує суспільству та державі. Протидія СБУ кримінальним правопорушенням на об'єктах КІ є частиною системи їх захисту від загроз, що поєднує правове регулювання та організаційні заходи діяльності сил та засобів СБУ. Однак чинне кримінальне законодавство, кримінальне процесуальне законодавство залишається фрагментарно врегульованим, бракує спеціальних норм для КІ, що ускладнює слідчу практику.

Протидія СБУ кримінальним посяганням на ОКІ займає особливе місце в загальній системі забезпечення національної безпеки України, становлячи один з ключових елементів комплексного підходу до захисту від кримінальних посягань на об'єкти критичної інфраструктури. Саме ця діяльність СБУ є частиною ширшої системи заходів, що охоплюють правове регулювання, фізичну охорону, технічне обладнання, кіберзахист, інформаційне реагування, моніторинг і прогнозування загроз, а також взаємодію між державними органами, органами місцевого самоврядування та приватними операторами критичної інфраструктури.

З огляду на зростання загроз від кримінальних посягань на об'єкти критичної інфраструктури, актуальною видається необхідність розроблення цілісної державної концепції протидії кримінальним правопорушенням на таких об'єктах. Така концепція має ґрунтуватися на міждисциплінарному, ризик-орієнтованому підході та охоплювати нормативно-правові, організаційно-процесуальні, технічні й кадрові механізми протидії. Її реалізація повинна забезпечити належне функціонування системи запобігання, виявлення, припинення та досудове розслідування кримінальних посягань на ОКІ, з урахуванням специфіки галузей, до яких належать такі об'єкти. Концепція має стати основою для подальшого вдосконалення кримінального законодавства, розроблення спеціалізованих методичних документів, а також забезпечення ефективної взаємодії між правоохоронними органами, суб'єктами національної безпеки і оборони та національної системи захисту критичної інфраструктури.

Перспективи подальших досліджень полягають у розроблені теоретичних, правових та організаційно-тактичних засад протидії СБУ кримінальним правопорушенням на ОКІ, адаптації міжнародних стандартів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Арсенович Л. Інструментарій підвищення рівня цифрової компетентності фахівців національної системи захисту критичної інфраструктури у публічному управлінні. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2024. № 2(74). С. 7–16. DOI: https://doi.org/10.32689/2523-4625-2024-2(74)-1.
2. Бажанов М. Науковий семінар з проблем боротьби з тероризмом та злочинами терористичної спрямованості. *Вісник Академії правових наук України*. 1998. № 4. С. 215.
3. Батюк О.В. Криміналістичне забезпечення протидії злочинам на об'єктах критичної інфраструктури: монографія. Луцьк: Гадяк Ж.В.: Волиньполіграф, 2021. 455 с.
4. Бєлай С.В., Євтушенко І.В., Мацюк В.В. Теоретико-методологічні засади підготовки кадрів у сфері захисту критичної інфраструктури України. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*. 2021. № 2. С. 342–350. URL: http://vdu-nuczu.net/ua/11-ukr/storinkaavtora/180-belaj-s-v-evtushenko-i-v-matsyuk-v-v-teoretiko-metodologichni-zasadi-pidgotovki-kadriv-u-sferi-zakhistu-kritichnoji-infrastrukturi-ukrajini (дата звернення: 27.06.2025).

5. Васильєв О.В. Методологія і практика інфраструктурного забезпечення функціонування і розвитку регіонів України: монографія. Харків : ХНАМГ, 2007. С. 23.
6. Делембовський М., Ткаченко В., Мельник Д. Захист критичної інфраструктури України від кібератак. *Grail of Science*. 2024. № 41. С. 277–281. DOI: https://doi.org/10.36074/grail-of-science.05.07.2024.043.
7. Довгань О.Д., Чернухін І.О. Організаційно-правові засади побудови системи захисту критичної інфраструктури від кібернетичних атак. *Інформаційна безпека людини, суспільства, держави*. 2012. № 2(9). С. 29–31.
8. Єфіменко І., Сліпченко В., Вашко А. Критична інфраструктура як об'єкт злочинного посягання: загальна характеристика й особливості організації розслідування. URL: https://lawscience.com.ua/uk/journals/tom-28-2-2023/kritichna-infrastruktura-yak-ob-yekt-zlochinnogo-posyagannya-zagalna-kharakteristika-y-osoblivosti-organizatsiyi-rozsliduvannya (дата звернення: 27.06.2025).
9. Зелена книга з питань захисту критичної інфраструктури в Україні: аналітична доповідь / Д.С. Бірюков та ін. Київ: НІСД, 2015. 35 с.
10. Ковалів М., Скриньковський Р., Назар Ю., Єсімов С., Красницький І., Кайдрович Х., Князь С., Кемська Ю. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. *Traektoriâ Nauki = Path of Science*. 2021. Vol. 7, № 4. С. 2011–2018.
11. Коваль М.В., Коваль В.В., Коцюруба В.І., Білик А.С. Організаційно-технічні засади побудови системи інженерного захисту об'єктів критичної інфраструктури енергетичної галузі України. *Наука і оборона*. 2023. С. 11–16.
12. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 27.06.2025).
13. Курбанов Я.Л. Забезпечення природно-техногенної безпеки в Україні і проблема визначення поняття «критична інфраструктура». *Південноукраїнський правничий часопис*. 2016. № 2. С. 151.
14. Кучерина С.Є., Олєйніков Д.О. Сучасний стан кримінально-правової охорони об'єктів критичної інфраструктури. *Інформація і право*. 2021. № 1. С. 90–98. URL: http://nbuv.gov.ua/UJRN/Infpr_2021_1_12 (дата звернення: 27.06.2025).
15. Лисенко А.М. Аналіз розвитку антитерористичного законодавства в Україні. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2011. № 4. С. 327–333. URL: http://nbuv.gov.ua/UJRN/Nvdduvs_2011_4_47 (дата звернення: 27.06.2025).
16. Ліпкан В.А. Кримінальний тероризм і система безпеки підприємства. *Недержавна система безпеки підприємства як суб'єкт національної безпеки України*. Київ: Вид-во Європейського ун-ту, 2001. С. 9.
17. Конвенція Ради Європи про запобігання тероризму : Міжнародний документ від 16.05.2005 р. № 994_838. URL: https://zakon.rada.gov.ua/laws/show/994_712#Text (дата звернення: 27.06.2025).
18. Новий словник іншомовних слів: близько 40 000 сл. і словосполучень / за ред. Л.І. Шевченко. Київ: АРІЙ, 2008. 672 с.
19. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 27.06.2025).
20. Рада Безпеки ООН ухвалила українську резолюцію та провела відкриті дебати щодо захисту критичної інфраструктури від терористичних атак. URL: https://mfa.gov.ua/news/54673-rada-bezpeki-oon-uhvalila-ukrajinsyku-rezolyuciju-ta-provela-vidkriti-debati-shhodo-zahistu-kritichnoji-infrastrukturi-vid-teroristichnih-atak (дата звернення: 27.06.2025).
21. Теленик С.С. Адміністративно-правове регулювання державної системи захисту критичної інфраструктури України. URL: http://phd.znu.edu.ua/page/dis/07_2021/Telenyk.pdf (дата звернення: 27.06.2025).
22. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 № 287/2015. URL: https://www.president.gov.ua/documents/2872015-19070 (дата звернення: 27.06.2025).
23. Черевко К., Пашнєв Д. Кібератаки на об'єкти критичної інфраструктури в умовах ведення війни: ключові поняття. *Вісник Кримінологічної асоціації України*. 2024. № 31(1). С. 209–219. DOI: https://doi.org/10.32631/vca.2024.1.15.
24. Чуницька І. І. Інфраструктура фінансового ринку України: поняття, функції, та еволюція статусу. *БІЗНЕСІНФОРМ*. 2014. № 9. С. 252.
25. Bubela T., Melnyk M., Nazarovets O., Rudyk Y. Аналіз визначень та нормативних вимог системи захисту об'єкта критичної інфраструктури. *Вісник Львівського державного університету без-*

пеки життєдіяльності. 2024. № 29. С. 119–127. DOI: https://doi.org/10.32447/20784643.29.2024.13.
26. 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 345/75. URL: https://eur-lex.europa.eu/eli/dir/2008/114/oj (дата звернення: 27.06.2025).
27. Critical Infrastructure Information Act of 2002 («CII Act»). URL: https://www.fas.org/sgp/crs/RL31762.pdf (дата звернення: 27.06.2025).
28. European Programme for Critical Infrastructure Protection. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:l33260 (дата звернення: 27.06.2025).
29. Hirschman A.O. National Power and the Structure of Foreign Trade. 1945.
30. Nurkse R. Trade and Development / Editors: R. Kattel, J.A. Kregel, E.S. Reinert. London, New York: Anthem, 2009. 504 p.
31. Rosenstain-Rodan P.N. The Notes of the Theory of the «Big Bush» in Economic Development for Latin America. London, New York, 1961.
32. Smetana M. Protection of critical infrastructure. Approaches of the European Union states to determination of critical infrastructure elements. HSB. Technical University of Ostrava, 2014/15.
33. Strahnitskyi Y. Institutional transformations in the direction of increasing the effectiveness of the state policy of critical infrastructure protection. *Public Administration and Regional Development*. 2024. № 23. P. 28–51. DOI: https://doi.org/10.34132/pard2024.23.02.
34. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT ACT) ACT OF 2001. URL: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm (дата звернення: 27.06.2025).