УДК 351.78
DOI https://doi.org/10.32782/2524-0374/2024-10/14

КРИМІНАЛЬНО-ПРАВОВИЙ АСПЕКТ ДОСЛІДЖЕННЯ ЗАГРОЗ КРИТИЧНІЙ ІНФРАСТРУКТУРІ ТА ЇЇ ОБ'ЄКТАМ

CRIMINAL LEGAL ASPECT OF THE STUDY OF THREATS TO CRITICAL INFRASTRUCTURE AND ITS OBJECTS

Предместніков О.Г., д.ю.н., професор,
заслужений юрист України, завідувач кафедри права
Мелітопольський державний педагогічний університет імені Богдана Хмельницького

Стаття присвячена критичній інфраструктурі як об'єкту пізнання. Визначається важливість критичної інфраструктури для забезпечення національної безпеки, стабільності економіки та обороноздатності держави. Аналізується законодавче регулювання у цій сфері, зокрема, Закон України «Про критичну інфраструктуру», який містить визначення та класифікацію ключових об'єктів та систем критичної інфраструктури. Розглянуто, як порушення функціонування цих об'єктів може спричиняти суспільно-небезпечні наслідки для суспільства та держави й тягти кримінальну відповідальність за тими чи іншими статтями КК України.

Порівняння із закордонним досвідом (США, ЄС, Великобританія, Китай, Японія) показує, що Україна враховує міжнародні підходи до захисту критичної інфраструктури, проте має свої унікальні особливості, зумовлені національними загрозами та викликами. У США, наприклад, критична інфраструктура визначається як системи та активи, настільки важливі, що їх нездатність функціонувати або руйнування матимуть руйнівний вплив на безпеку, національну економіку, громадське здоров'я або безпеку. Європейський Союз підходить до цього питання через Директиву про європейські критичні інфраструктури, акцентуючи на взаємозв'язку та координації між державами-членами. Велика Британія приділяє велику увагу кібербезпеці, а Китай та Японія акцентують на національному контролі та стійкості об'єктів.

На основі проведеного аналізу надано рекомендації для удосконалення законодавчої політики України у сфері критичної інфраструктури. Зокрема, пропонується уведення в КК України розділу, присвяченого злочинам проти критичної інфраструктури. Окремо акцентується увага на необхідності наукових досліджень у сфері кібербезпеки та оцінки ризиків для розробки ефективних стратегій захисту. Таким чином, стаття робить внесок у розуміння актуальних питань правової охорони критичної інфраструктури та надає практичні рекомендації для подальшого вдосконалення цієї сфери.

Ключові слова: критична інфраструктура, національна безпека, законодавство, кібербезпека, категорії критичності, Україна.

The article delves into the main aspects of legal protection of critical infrastructure objects in Ukraine. It underscores the importance of critical infrastructure in ensuring national security, economic stability, and the defense capability of the state. The legislative regulation in this sphere, particularly the Law of Ukraine "On Critical Infrastructure," is analyzed, providing definitions and classifications of key critical infrastructure objects and systems. The article examines how disruptions in the functioning of these objects can lead to significant negative consequences for society and the state. The categorization of critical infrastructure objects into criticality categories is also analyzed, which allows for more efficient planning and implementation of protective measures, directing resources to the most important and vulnerable objects.

A comparison with international experience (USA, EU, UK, China, Japan) shows that Ukraine considers international approaches to critical infrastructure protection but has its unique features determined by national threats and challenges. For instance, in the USA, critical infrastructure is defined as systems and assets so vital that their inability to function or destruction would have a devastating impact on security, the national economy, public health, or safety. The European Union approaches this issue through the Directive on European Critical Infrastructures, emphasizing interconnection and coordination among member states. The UK pays great attention to cybersecurity, while China and Japan emphasize national control and the resilience of objects.

Based on the conducted analysis, recommendations are provided for improving Ukraine's legislative policy in the field of critical infrastructure. Specifically, the development of more detailed regulatory acts, strengthening coordination among various agencies, and the implementation of new technologies to in the field of cybersecurity and risk assessment to develop effective protection strategies. Thus, the article makes a significant contribution to ensure the resilience of critical infrastructure are proposed. Particular attention is given to the necessity of scientific research understanding current issues in the legal protection of critical infrastructure and provides practical recommendations for further improvement in this area.

Key words: critical infrastructure, national security, legislation, cybersecurity, criticality categories, Ukraine.

Постановка проблеми. Критична інфраструктура є однією з найважливіших складових сучасного суспільства, яка забезпечує нормальне функціонування державних інститутів, економічних систем та життєдіяльність населення. В умовах глобалізації та стрімкого технологічного розвитку, важливість захисту критичної інфраструктури від різноманітних загроз значно зросла. Загрози, які можуть бути спрямовані на об'єкти критичної інфраструктури, включають як традиційні ризики, пов'язані з природними катастрофами та техногенними аваріями, так і нові виклики, такі як кіберзагрози, терористичні атаки та гібридні війни.

Актуальність дослідження критичної інфраструктури та загроз її об'єктам зумовлена необхідністю розробки ефективних правових механізмів та стратегій для забезпечення її захисту. Зокрема, це стосується не тільки державної безпеки, а й забезпечення безперервного функціонування економічних та соціальних систем, що є ключовими для стабільного розвитку держави.

У сучасних умовах, коли світ стає все більш взаємозалежним, а технологічний прогрес невпинно рухається вперед, наукове пізнання загроз критичної інфраструктури набуває нових аспектів. Це потребує міждисциплінарного підходу, що включає аналіз правових, економічних, соціальних та технологічних аспектів, а також інтеграцію досвіду різних країн та міжнародних організацій.

Аналіз останніх досліджень. Вже досить тривалий час критична інфраструктура перебуває в полі зору вітчизняних дослідників. Так, О. Верголяс наголошує на необхідності глибоких реформ у сфері захисту критичної інфраструктури України. Він вказує на важливість інтеграції новітніх технологій та підходів для забезпечення безпеки ключових об'єктів, особливо у контексті зростання гібридних загроз [1]. Це твердження знаходить підтримку у дослідженні І. В. Гори та О. В. Батюка, які розглядають закордонний досвід у сфері захисту об'єктів критичної інфраструктури. Вони підкреслюють, що багато країн вже давно впроваджують інноваційні методи для підвищення стійкості своїх критичних об'єктів [2, с. 132].

Подібний акцент на міжнародний досвід робить і О. П. Єрменчук, аналізуючи основні підходи до організації захисту критичної інфраструктури в країнах Європи. Єрменчук звертає увагу на те, що систематичний підхід до планування та виконання заходів безпеки є ключовим

елементом успіху у цій сфері [3, с. 45]. Аналізуючи ці підходи, Д. С. Бірюков та С. І. Кондратов також зазначають, що для України важливо враховувати рекомендації міжнародних експертів та адаптувати їх до національних умов [4, с. 21].

Г. Каніщев та І. Тур зосереджуються на критичній інфраструктурі тимчасово окупованих територій України, звертаючи увагу на прогалини в українському законодавстві, які потребують негайного вирішення для забезпечення безпеки цих територій [5, с. 18]. Водночас С. Кондратов аналізує проблеми правового та організаційного забезпечення протидії тероризму, що також є важливим аспектом захисту критичної інфраструктури [6, с. 19].

Поняття критичної інфраструктури та його визначення у науковій літературі досліджується І. В. Урядніковою та В. М. Заплатинським. Вони наголошують на необхідності чіткого визначення термінології для ефективного управління та захисту критичних об'єктів [9, с. 184]. С. С. Теленик, розглядаючи адміністративно-правове регулювання критичної інфраструктури, підкреслює, що правова основа є необхідною для розробки ефективних заходів безпеки [8, с. 15].

Загальні проблеми організаційно-нормативного характеру у сфері безпеки критичної інфраструктури в Україні аналізуються В. І. Франчуком, П. Я. Пригуновим та С. І. Мельником. Вони вказують на те, що впровадження комплексного підходу до захисту критичних об'єктів є необхідним для забезпечення стійкості та безпеки держави [10, с. 142].

Таким чином, огляд літератури свідчить про значну увагу до проблем захисту критичної інфраструктури як на національному, так і на міжнародному рівнях. Узагальнюючи думки дослідників, можна зробити висновок про важливість інтеграції міжнародного досвіду, системного підходу та правового забезпечення для ефективного захисту критичної інфраструктури України.

Мета дослідження полягає в аналізі критичної інфраструктури як об'єкта правового захисту, визначенні основних загроз, що можуть негативно вплинути на її функціонування та потягти кримінальну відповідальність відповідно до КК України У контексті глобальних викликів та регіональних особливостей, особлива увага приділяється вивченню досвіду інших країн у забезпеченні захисту критичної інфраструктури та можливості його адаптації до українських реалій.

Таким чином, стаття спрямована на поглиблене розуміння проблематики кримінально-правової охорони критичної інфраструктури та створення науково обґрунтованих рекомендацій для зміцнення безпеки та стабільності держави в умовах сучасних загроз та викликів.

Виклад основного матеріалу.

1. Поняття критичної інфраструктури за законодавством України та закордонних країн: зіставний аспект. Критична інфраструктура є фундаментально важливим елементом забезпечення національної безпеки України, що знайшло своє закріплення в Законі України «Про критичну інфраструктуру» (№ 1882-IX від 16 листопада 2021 року). Визначення критичної інфраструктури у цьому законі охоплює сукупність об’єктів, систем, їх частин та сукупностей, що є ключовими для економіки, національної безпеки і оборони країни. Ці об’єкти та системи повинні мати можливість функціонувати безперервно та ефективно, а їх порушення може мати серйозні наслідки для національних інтересів, суспільства та держави. Закон України «Про критичну інфраструктуру» в статті 1 визначає критичну інфраструктуру як сукупність об’єктів, систем, їх частин та сукупностей, що забезпечують життєво важливі функції та послуги, безпеку яких необхідно захищати від загроз природного, техногенного, технологічного чи людського характеру.

Порівнюючи з міжнародним досвідом визначення критичної інфраструктури виявляються цікаві подібності й відмінності. Наприклад, в США, критична інфраструктура визначається у секції 1016 (e) «Патріотичного акту США» (Patriot Act) як системи та активи, фізичні або віртуальні, настільки важливі для Сполучених Штатів, що їх нездатність функціонувати або руйнування матимуть руйнівний вплив на безпеку, національну економіку, громадське здоров’я або безпеку. Законодавство США звертає увагу на захист від терористичних загроз, кіберзагроз та інших небезпек, що можуть мати масштабний вплив на країну.

Європейський Союз визначає критичну інфраструктуру в Директиві про європейську критичну інфраструктуру (Directive 2008/114/EC), де вона визначається в статті 2 як об’єкти та системи, важливі для збереження життєво важливих суспільних функцій, здоров’я, безпеки, економічного або соціального добробуту людей, де збій у роботі або руйнування матимуть серйозні наслідки для принаймні двох держав-членів. ЄС акцентує на взаємозв’язку та координації між державами-членами в питаннях захисту критичної інфраструктури.

У Сполученому Королівстві критична інфраструктура визначається в Національній стратегії кібербезпеки Великобританії (UK National Cyber Security Strategy) як ті елементи, системи та мережі, які є необхідними для функціонування суспільства та економіки країни. Це охоплює такі елементи, як: енергетику, воду, транспорт, охорону здоров’я, комунікації та фінансові послуги. Великобританія також приділяє велику увагу кібербезпеці як ключовому аспекту захисту критичної інфраструктури.

Китайська Народна Республіка визначає критичну інфраструктуру у Законі про національну безпеку КНР (中华人民共和国国家安全法) як об’єкти, що є основою для забезпечення національної безпеки, економічного розвитку, соціальної стабільності та добробуту населення. Китайський підхід охоплює широкий спектр секторів, включаючи енергетику, транспорт, водопостачання, телекомунікації, фінанси та оборону, акцентуючи на важливості національного контролю та захисту від іноземних загроз.

Японія також має своє визначення критичної інфраструктури у Законі про захист життєво важливої інфраструктури (重要インフラ保護法), під якою розуміються об’єкти та системи, необхідні для забезпечення життєдіяльності країни, зокрема у сфері енергетики, транспорту, зв’язку, охорони здоров’я та фінансів. Японський підхід наголошує на важливості стійкості та відновлюваності цих об’єктів у разі надзвичайних ситуацій.

Таким чином, українське законодавство про критичну інфраструктуру в багатьох аспектах відображає міжнародний досвід, проте має свої унікальні особливості, зумовлені специфікою національних загроз та викликів. Порівняння із законодавством інших країн демонструє як загальні підходи до забезпечення безпеки та стійкості критичної інфраструктури, так і унікальні рішення, що враховують конкретні національні умови.

Аналізуючи підходи різних країн до визначення критичної інфраструктури, можна зазначити, що кожна країна визначає цей термін виходячи зі своїх національних інтересів та пріоритетів. Наприклад, США приділяють особливу увагу кібербезпеці та захисту від терористичних загроз, що відображає їхній досвід боротьби з тероризмом та кіберзлочинністю. Європейський Союз акцентує на координації між державами-членами, що є логічним з огляду на політичну та економічну інтеграцію в ЄС. Британія, як і США, приділяє велику увагу кібербезпеці, враховуючи швидкий розвиток технологій та залежність від них. Китай зосереджується на національному контролі та захисті від іноземних загроз, що відображає політичну та економічну стратегію країни. Японія наголошує на стійкості та відновлюваності критичної інфраструктури у разі надзвичайних ситуацій, що враховує їхній досвід з природними катастрофами.

Зі свого боку, українське законодавство відображає прагнення до гармонізації з міжнародними стандартами, враховуючи при цьому специфіку національних умов. Закон України «Про критичну інфраструктуру» забезпечує правову основу для захисту життєво важливих об'єктів та систем, що є необхідним для національної безпеки та стабільності. Цей закон також враховує загрози, що можуть бути природного, техногенного, технологічного чи людського характеру, що робить його комплексним та адаптивним до різних видів ризиків.

2. Загроза об'єктам критичної інфраструктури: кримінально-правовий аспект. Важливість об'єктів критичної інфраструктури (ОКІ) для кожної держави вимагає також створення дієвої системи кримінально-правової протидії відповідним порушенням стосовно відповідних об'єктів.

Важливо відзначити, що КК України не послуговується словосполученням «об'єкти критичної інфраструктури», відповідно, їхня кримінально-правова охорона здійснюється з використанням не однієї, а цілої низки норм:

1) Умисне знищення чи пошкодження майна (ст. 194 КК України). Стаття 194 Кримінального кодексу України передбачає кримінальну відповідальність за умисне знищення чи пошкодження майна. У контексті охорони об'єктів критичної інфраструктури ця норма є базовою, оскільки охоплює будь-яке майно, як рухоме, так і нерухоме. Основним об'єктом злочину є право власності, але додатковими об'єктами можуть виступати громадський порядок, екологічна безпека, життя і здоров'я людини.

2) Умисне пошкодження об'єктів електроенергетики (ст. 194-1 КК України). Ця стаття передбачає кримінальну відповідальність за умисне пошкодження або руйнування об'єктів електроенергетики, що є критично важливими для функціонування інфраструктури держави. Зокрема, пошкодження таких об'єктів може призвести до перебоїв у постачанні електроенергії, що своєю чергою може негативно вплинути на інші важливі системи, включаючи охорону здоров'я, транспорт та зв'язок. Відповідно до п. 1 ч. 1 ст. 6 Закону України «Про основні засади забезпечення кібербезпеки», такі об'єкти віднесені до критичної інфраструктури, і їх пошкодження кваліфікується за ст. 194-1 КК України.

3) Диверсія (ст. 113 КК України). Стаття 113 КК України передбачає відповідальність за диверсію, тобто дії, спрямовані на ослаблення держави шляхом пошкодження чи знищення об'єктів, що мають важливе народногосподарське чи оборонне значення. У контексті об'єктів критичної інфраструктури ця норма є особливо важливою, оскільки такі об'єкти безпосередньо впливають на національну безпеку та оборону. Диверсія може включати пошкодження об'єктів енергетики, транспорту, зв'язку та інших ключових систем, що забезпечують життєдіяльність країни.

4) Терористичний акт (ст. 258 КК України). Терористичний акт, визначений у ст. 258 КК України, включає посягання на об'єкти критичної інфраструктури з метою порушення громадської безпеки, залякування населення або впливу на прийняття рішень державними органами. Об'єкти критичної інфраструктури є привабливими цілями для терористів через їх важливість для нормального функціонування суспільства та економіки. Наприклад, пошкодження енергетичних станцій, водопостачальних систем чи транспортних вузлів може мати катастрофічні наслідки для безпеки та стабільності країни.

Розмежування злочинів на об'єкті критичної інфраструктури, коли вони є диверсією, а коли терористичним актом, є важливим аспектом кримінального права. Для цього необхідно звернути увагу на об'єктивні та суб'єктивні ознаки складів злочинів, передбачених статтями 113 та 258 Кримінального кодексу України.

Об'єктивними ознаками диверсії є дії, спрямовані на пошкодження або знищення об'єктів критичної інфраструктури, а суб'єктивними ознаками – мета ослаблення держави та намір спричинити значні матеріальні збитки чи інші негативні наслідки для держави.

Натомість терористичний акт, визначений у статті 258 КК України, включає посягання на об'єкти критичної інфраструктури з метою порушення громадської безпеки, залякування населення або впливу на прийняття рішень державними органами. Об'єктивними ознаками терористичного акту є вчинення вибуху, підпалу або інших дій, які створюють небезпеку для життя чи здоров'я людей, а суб'єктивними ознаками – мета порушення громадської безпеки, залякування населення та намір впливу на прийняття рішень органами державної влади.

Основна відмінність між диверсією та терористичним актом полягає у меті. Диверсія спрямована на ослаблення держави, підрив її економічної чи оборонної потужності. Натомість терористичний акт має на меті порушення громадської безпеки, залякування населення або вплив на рішення державних органів. Спосіб вчинення також відрізняється: терористичні акти часто пов'язані з використанням насильницьких методів, що створюють загрозу для життя людей, таких як вибухи чи підпали. Диверсія може включати дії, що спрямовані на пошкодження стратегічних об'єктів без прямої загрози життю людей. Важливим є також аналіз наслідків для держави: диверсія має на меті безпосереднє ослаблення державних інститутів через знищення або пошкодження критично важливих об'єктів інфраструктури, тоді як терористичний акт спрямований на створення страху, паніки серед населення та дестабілізацію суспільного порядку.

Для ілюстрації цього розмежування можна навести приклади. Якщо особа здійснила підрив стратегічного мосту, який використовується для військових перевезень, з метою ослаблення оборонної здатності держави, то це є диверсією, оскільки мета – підрив оборонної потужності держави. Якщо ж особа здійснила вибух у громадському місці, щоб залякати населення та змусити уряд виконати певні політичні вимоги, то це є терористичним актом, оскільки мета – залякування населення та вплив на рішення уряду.

Таким чином, для правильного розмежування диверсії та терористичного акту необхідно ретельно аналізувати мету та обставини вчинення злочину, враховуючи як об'єктивні, так і суб'єктивні ознаки.

5) Напад на об'єкти, на яких є предмети, що становлять підвищену небезпеку для оточення (ст. 261 КК України). Стаття 261 КК України передбачає відповідальність за напад на об'єкти, на яких зберігаються, використовуються або транспортуються радіоактивні, хімічні, біологічні чи вибухонебезпечні матеріали. У контексті критичної інфраструктури, такі об'єкти є особливо важливими через їх потенційну небезпеку для населення та навколишнього середовища. Напад на такі об'єкти може спричинити серйозні аварії або катастрофи, що вимагатиме негайного реагування з боку державних служб і може мати довгострокові негативні наслідки.

6) Пошкодження шляхів сполучення і транспортних засобів (ст. 277 КК України). Стаття 277 КК України встановлює відповідальність за пошкодження шляхів сполучення, транспортних засобів, споруд чи засобів зв'язку. У випадку критичної інфраструктури, це може включати дороги, мости, залізниці, аеропорти та морські порти, що є ключовими для транспортування товарів та людей. Пошкодження таких об'єктів може спричинити перебої у постачанні ресурсів, порушення економічної діяльності та створення загроз для життя і здоров'я людей.

З наведеного аналізу КК України вбачається, що об'єкти критичної інфраструктури *не розглядаються як окремий об'єкт чи складова об'єкта злочину.* Спроба систематизувати кримінально-правову охорону відповідних об'єктів була запроваджена Законом № 2997-IX від 21 березня

2023 року, яким було доповнено статтю 258-6 приміткою, що пояснює вживання словосполучення «критично важливі об'єкти інфраструктури». Так, в означеній статті містить відсильна норма, згідно з якою останній термін тут вжито у значенні, визначеному Законом України «Про основні засади забезпечення кібербезпеки України». Згідно з пунктом 19 частини 1 статті 1 цього закону об'єкт критичної інформаційної інфраструктури визначається як комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури. З цього також випливає, що норми КК України, що забезпечують кримінально-правову охорону об'єктів критичної інфраструктури, (а) ані генетично, ані функціонально не пов'язані з відповідними нормами Закону України «Про критичну інфраструктуру», (б) не забезпечують системного (а отже й цілісного, уніфікованого) підходу до захисту об'єктів критичної інфрастуктури.

Окрім того, через непов'язаність чинної редакції КК України із законом України «Про критичну інфраструктуру» виникає питання про те, чи можна в кримінально-правовій кваліфікації тих чи інших посягань на об'єкти критичної інфраструктури використовувати поділ таких об'єктів за рівнем їхньої критичності (1–4). Гадаємо, що цих та подібних ускладнень можна було б уникнути через запровадження системної кримінально-правової охорони об'єктів критичної інфраструктури в КК України.

Висновки. Проведений аналіз свідчить про те, що рівень кримінально-правової охорони об'єктів критичної інфраструктури в Україні наразі є недостатнім і безсистемним. Це обумовлено кількома ключовими факторами.

По-перше, чинне законодавство не враховує сучасний розвиток організаційно-правових засад критичної інфраструктури, що призводить до втрати здатності повною мірою охороняти інтереси держави і суспільства, які реалізуються через можливості критичної інфраструктури. Законодавство, яке встановлює кримінальну відповідальність за суспільно небезпечні діяння, не має індивідуалізованого підходу до критичної інфраструктури взагалі та її об'єктів зокрема.

По-друге, кримінально-правова охорона об'єктів критичної інфраструктури здійснюється через різні кримінально-правові норми, які розміщені в різних розділах Кримінального кодексу України. Таке розпорошення норм не забезпечує системного підходу до захисту критичної інфраструктури, що може призвести до формування неоднорідної слідчо-судової практики.

По-третє, законодавство про кримінальну відповідальність не враховує деякі сучасні загрози, зокрема кіберзагрози, що є критичними для захисту інформаційної інфраструктури об'єктів критичної інфраструктури. Це підкреслює необхідність впровадження спеціальних норм, що забезпечували б охорону об'єктів критичної інформаційної інфраструктури.

З огляду на вищевикладене, пропонується створити єдину систему кримінально-правової охорони об'єктів критичної інфраструктури, яка б забезпечувала комплексний підхід до їхнього захисту. Останнє включає введення в КК України окремого розділу, присвяченого злочинам проти об'єктів критичної інфраструктури.

Ми також переконані у необхідності проводити подальші наукові дослідження в сфері кібербезпеки та оцінки ризиків для розробки ефективних стратегій кримінально-правової протидії злочинам означеної категорії.

ЛІТЕРАТУРА

1. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз. [Електронний ресурс]. URL: https://coolyanews.info/reformuvannyasistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriiziiaktual.html
2. Гора І.В., Батюк О.В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії*. 2021. № 4(1), 132–139. URL: https://doi.org/10.32518/2617-4162-2021-1-132-139
3. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.
4. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. міжнар. експерт. нарад / упоряд. Д.С. Бірюков, С.І. Кондратов ; за заг. ред. О.М. Суходолі. К. : НІСД, 2016. 176 с.
5. Каніщев Г., Тур І. Критична інфраструктура тимчасово окупованих територій України в українському законодавстві. Міждисциплінарний дискурс: стійкість критичної інфраструктури [Електронний ресурс] : тези доповідей науково-практичної конференції, 14 травня 2024 року. – Харків : ХАІ, 2024. С. 69–73. URL: https://dspace.library.khai.edu/xmlui/bitstream/handle/123456789/7292/Mizhdystsyplinarnyy_dyskurs.pdf?sequence=1&isAllowed=y#page=69
6. Кондратов С. Про деякі проблеми правового та організаційного забезпечення протидії тероризму на сучасному етапі. *Державна політика протидії тероризму: пріоритети та шляхи реалізації : зб. матеріалів «круглого столу»*. К. : НІСД, 2011. С. 18–22. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf.
7. Закон України «Про критичну інфраструктуру» із змінами від № 1909-IX від 18.11.2021. *Відомості Верховної Ради* (ВВР), 2023, № 5, ст. 13. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
8. Теленик С.С. Критична інфраструктура як об'єкт адміністративно-правового регулювання. *Юридичний часопис Національної академії внутрішніх справ*. 2018. № 1 (15). URL: http://elar.naiau.kiev.ua/bitstream/123456789/6663/1/17.pdf.
9. Уряднікова І.В., Заплатинський В.М. *Наукові* підходи до визначення терміну «критична інфраструктура». *Вісті Донецького гірничого інституту*. 2020. №2 (47). URL: https://doi.org/10.31474/1999-981X-2020-2-184-193.
10. Франчук В.І., Пригунов П.Я., Мельник С.І. Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії.* 2021. № 3 (13). С. 142–148. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf.