УДК 343.9:004:351.78:327.54
DOI https://doi.org/10.24144/2307-3322.2024.84.3.39

ЗАГРОЗИ ОБ'ЄКТАМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

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

Герасименко О.М. Загрози об'єктам критичної інфраструктури України в умовах воєнного стану.

Стаття присвячена аналізу загроз критичній інфраструктурі України. Актуальність дослідження зумовлена небезпечною динамікою рівня загроз, які впливають на національну безпеку та соціально-економічну стабільність держави в умовах воєнного стану. Аналіз наукової літератури показав, що на сьогоднішній день відсутній єдиний підхід до класифікації та оцінки таких загроз. З огляду на це, мета статті – проаналізувати існуючі класифікації загроз критичній інфраструктурі та запропонувати авторську класифікації їх проявів на об'єктах критичної інфраструктури в умовах воєнного стану з урахуванням зарубіжного та національного досвіду.

В процесі дослідження виконано низку завдань: визначено сутність понять «загроза критичній інфраструктурі»; здійснено аналіз правових документів щодо захисту критичної інфраструктури; вивчено вітчизняний та зарубіжний досвід класифікації загроз; розглянуто принципи, на яких базуються вітчизняні й зарубіжні класифікації та оцінено їх ефективність; розроблено власну класифікацію загроз критичній інфраструктурі для України.

За результатами дослідження встановлено, що на сьогоднішній день існують різні класифікації загроз критичній інфраструктурі. Однак, на нашу думку, дієвою та такою, що відповідає сучасним викликам є класифікація, яка враховує всі форми їх прояву: фізичні посягання, кібератаки, економічні диверсії, терористичні дії, посягання з використання кліматичної зброї та ін. Така класифікація загроз критичній інфраструктурі України є розробленою з урахуванням міжнародного та вітчизняного досвіду й має важливе значення для підвищення рівня національної безпеки, адже її користь полягає у систематизації теоретичних знань та поглибленому аналізі сучасних загроз, з якими стикається держава. Основна наукова цінність запропонованої класифікації полягає в її здатності інтегрувати різні аспекти загроз у єдину класифікацію, що враховує як внутрішні, так і зовнішні фактори, таким чином вона дозволяє більш точно оцінити ризики та запровадити відповідні заходи для захисту об'єктів національної критичної інфраструктури.

Ключові слова: критична інфраструктура, загроза критичній інфраструктурі, національна безпека, економічна стабільність, кіберзагроза.

Herasymenko O.M. Threats to critical infrastructure objects of Ukraine under martial law.

The article is devoted to analyzing threats to Ukraine's critical infrastructure. The relevance of the study is driven by the dangerous dynamics of threat levels that affect national security and the socio-economic stability of the state under martial law. A review of the scientific literature revealed that there is currently no unified approach to the classification and assessment of such threats. Therefore, the article aims to analyze existing classifications of threats to critical infrastructure and propose an original classification of their manifestations on critical infrastructure objects under martial law, considering both international and national experiences.

During the research, several tasks were accomplished: the essence of the term «threat to critical infrastructure» was defined; an analysis of legal documents related to the protection of critical infrastructure was conducted; domestic and international experiences in threat classification were studied; principles underlying both domestic and foreign classifications were reviewed and their

effectiveness was assessed; and an original classification of threats to critical infrastructure for Ukraine was developed.

The results of the study revealed that there are various classifications of threats to critical infrastructure today. However, in our opinion, the most effective classification that meets modern challenges is one that considers all forms of their manifestations: physical assaults, cyberattacks, economic sabotage, terrorist actions, and assaults using climate weapons. This classification of threats to Ukraine's critical infrastructure is developed based on international and domestic experience and is of great importance for enhancing national security, as its value lies in the systematization of theoretical knowledge and a deep analysis of modern threats facing the state. The main scientific value of the proposed classification lies in its ability to integrate different aspects of threats into a single classification that takes into account both internal and external factors. This allows for a more accurate risk assessment and the implementation of appropriate measures to protect national critical infrastructure objects.

Key words: critical infrastructure, threat to critical infrastructure, national security, economic stability, cyber threat.

Постановка проблеми. Події останнього десятиліття в Україні, а також введення у 2022 році воєнного стану, призвели до зростання загальної кількості загроз, які спричиняють нанесення шкоди національній безпеці та обороні, соціально-економічному стану держави та іншим національним інтересам України. Серед загроз в умовах воєнного стану одними з небезпечних наразі є кримінальні правопорушення, що шкодять об'єктам транспортної мережі, електроенергетичної галузі, системи водопостачання, інформаційно-комунікаційної системи та ін. Прояви наведеної категорії загроз мають високу динаміку, а їх реалізація призводить до тяжких наслідків економічного, оборонного характеру, зростання соціальної напруги в суспільстві. В цих умовах набуває актуальності питання розробки системи класифікації загроз об'єктам критичної інфраструктури в умовах воєнного стану, що на нашу думку, сприятиме підвищенню ефективності протидії ним. Розв'язання зазначеної проблеми науковим шляхом також сприятиме удосконаленню правових та організаційних заходів протидії цим загрозам.

Враховуючи зазначене вище, а також значення критичної інфраструктури для забезпечення національної безпеки України, проведення наукового дослідження визначеного назвою статті є актуальним, своєчасним і таким, що є продовженням існуючої наукової дискусії відповідної сфери знань.

Стан опрацювання проблематики. Проблеми національної критичної інфраструктури, як ключового елементу національної безпеки, тривалий час привертають увагу науковців, які досліджують різні аспекти її захисту. Наукова дискусія відбувається навколо питань вивчення основних загроз для критичної інфраструктури та способів ефективної протидії їм. Серед зазначених відзначаємо дослідження О.О. Верголяса (2020 р.), який зосередився на визначенні критичної інфраструктури в контексті різних секторів, включаючи енергетику, хімічну промисловість, транспорт, фінанси, телекомунікації, харчування, охорону здоров'я та комунальні послуги. Його дослідження визначає ці сектори як стратегічно важливі для функціонування економіки та безпеки сфер держави. Автор акцентує увагу на необхідності глибоких реформ організації 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 [5].

І.В. Уряднікова та В.М. Заплатинський провели (2020 р.) дослідження, присвячене визначенню сутності критичної інфраструктури як сукупності фізичних і віртуальних систем, об'єктів та ресурсів, руйнування яких створює значні загрози національній безпеці, здоров'ю та безпеці населення [6].

Д.Г. Бобро в своєму досліджені (2015 р.) запропонував розглядати загрози для критичної інфраструктури, як існуючі та потенційно можливі явища і чинники, які становлять небезпеку для стійкого функціонування об'єктів критичної інфраструктури. Він акцентує увагу на техногенних аваріях та технічних збоях, часто спричинених людськими помилками, стихійними лихами та зловмисними діями [8].

О.М. Суходоля за результатами проведеного (2016 р.) дослідження визначив ключові загрози для критичної інфраструктури, такі як надзвичайні ситуації (стихійні лиха та техногенні аварії), терористичні акти, диверсії та кіберзагрози. Він звертає увагу на зростаючу складність і частоту

цих загроз, що підкреслює необхідність комплексного підходу для їхнього запобігання та мінімізації [15].

Автори «Зеленої книги з питань захисту критичної інфраструктури» Д.С. Бірюков, С.І. Кондратов, О.І. Насвіт, О.М. Суходоля здійснили (2015 р.) всебічний аналіз загроз, пов'язаних із аваріями, небезпечними природними явищами та зловмисними діями. Вони підкреслили необхідність системного підходу до захисту критичної інфраструктури, враховуючи як традиційні, так і нові виклики [9].

Подібний акцент на міжнародний досвід робить і О.П. Єрменчук, аналізуючи (2018 р.) основні підходи до організації захисту критичної інфраструктури в країнах Європи. Автор звертає увагу на те, що систематичний підхід до планування та виконання заходів безпеки є ключовим елементом успіху у цій сфері [10].

Зазначені вище дослідження створили наукову основу для подальшого вивчення загроз критичній інфраструктурі України та розробки ефективних заходів для її захисту. Однак, незважаючи на це, багато питань залишаються недостатньо вивченими. Зокрема, на сьогоднішній день відсутній єдиний підхід до класифікації та оцінки таких загроз.

Мета дослідження – проаналізувати існуючі класифікації загроз критичній інфраструктурі та запропонувати авторську класифікації їх проявів на об'єктах критичної інфраструктури в умовах воєнного стану з урахуванням зарубіжного та національного досвіду.

Виклад основного матеріалу. Регулювання правових та організаційних засад створення та функціонування національної системи захисту критичної інфраструктури здійснюється на основі ряду нормативно-правових актів [1].

«Кодекс системи передачі електроенергії» визначає критичну інфраструктуру як мережу об'єктів або компонентів Об'єднаної енергетичної системи України (ОЕС), необхідних для підтримки життєво важливих функцій суспільства, здоров'я, безпеки та добробуту громадян. Порушення або знищення цих об'єктів суттєво впливає на національну безпеку, навколишнє середовище, призведе до значних фінансових та людських втрат [2].

Закон України «Про критичну інфраструктуру» дає досить стисле визначення критичної інфраструктури, наголошуючи на її важливому значенні для економіки, національної безпеки та оборони. Він описує критичну інфраструктуру як об'єкти, системи або їх компоненти, порушення яких може завдати шкоди життєво важливим національним інтересам [3].

Подібним чином, Директива Ради 2008/114/ЕС описує критичну інфраструктуру як будь-який об'єкт, систему або її частину в державах-членах, які мають вирішальне значення для підтримки основних громадських функцій, здоров'я, безпеки або економічного та соціального добробуту. Пошкодження або руйнування такої інфраструктури матиме глибокий вплив на здатність держави-члена підтримувати ці функції [4].

Вітчизняний дослідник О.О. Верголяс визначає критичну інфраструктуру як підприємства та установи в різних секторах, включаючи енергетику, хімічну промисловість, транспорт, фінанси, телекомунікації, харчування, охорону здоров'я та комунальні послуги. Зазначені сектори визначає стратегічно важливими для функціонування економіки та безпеки держави. Автор робить висновок, що реальний вплив загроз призведе до порушення стабільності об'єктів критичної інфраструктури та нанесення шкоди для національної та громадської безпеки [5].

На думку І.В. Уряднікової та В.М. Заплатинського, критична інфраструктура включає фізичні та віртуальні системи, об'єкти та ресурси. Знищення або пошкодження цих елементів призводить до нанесення шкоди національній безпеці, здоров'ю та безпеці населення [6].

Що стосується терміну «загроза», то він визначається в Законі України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII як явища, тенденції та чинники, що роблять неможливою чи ускладнюють реалізацію національних інтересів та збереження національних цінностей України [7]. У контексті захисту критичної інфраструктури Д.Г. Бобро пропонує розглядати «загрозу» як існуючі та потенційно можливі явища і чинники, які становлять загрозу стійкому функціонуванню об'єктів критичної інфраструктури і можуть призвести до різних негативних наслідків [8]. Майже ідентичне формулювання зазначеного терміну міститься у Зеленій книзі з питань захисту критичної інфраструктури Д.С. Бірюкова, С.І Кондратова, О І. Насвіта, О.М. Суходолі, де під ним розуміються будь-які обставини або події, які можуть порушити стійке функціонування або знищити критичну інфраструктуру чи її елемент, а також будь-які спроби та наміри завдати шкоди критичним активам [9]. Аналогічне визначення дає О.П. Єрменчук, який розуміє

під загрозами критичній інфраструктурі існуючі або потенційно можливі явища та чинники, які можуть завдати шкоди такому об'єкту, вивести його з ладу або порушити функціонування відповідно до його призначення, тим самим поставивши під загрозу життєво важливі національні інтереси держави [10].

Виходячи з визначень, які наводяться в українському законодавстві та роботах вітчизняних дослідників, критичну інфраструктуру можна визначити як комплексну систему, що складається з об'єктів, систем і ресурсів, життєво важливих для функціонування держави. Це інфраструктура, відмова якої або її знищення можуть призвести до нанесення значної шкоди економіці, національній безпеці та обороні, соціальній безпеці. У свою чергу, загрозу критичній інфраструктурі необхідно розуміти як існуючі або потенційно можливі явища і чинники, що можуть порушити стійке функціонування або знищити об'єкт критичної інфраструктури або будь-який її елемент, а також будь-які спроби та наміри завдати шкоди критичним активам.

Проаналізуємо існуючі класифікації загроз критичній інфраструктурі та на основі цього аналізу запропонуємо авторську класифікацію загроз. Таке дослідження є важливим для розробки ефективних заходів протидії та захисту критичної інфраструктури України в сучасних умовах.

Зарубіжний досвід

У різних країнах спектр загроз критичній інфраструктурі та зміст поняття загроз визначаються індивідуально з урахуванням безпекової ситуації та пріоритетів державної політики.

США. У США загрози для критичної інфраструктури розуміються як природні або техногенні явища, суб'єкти чи дії, що становлять потенційну шкоду для життя, інформації, операцій, навколишнього середовища, власності. Основні загрози включають кібератаки, терористичні атаки та природні лиха.

ЄС. Європейський Союз визначає загрози критичній інфраструктурі через принципи та інструменти Європейської програми захисту критично важливої інфраструктури (EPCIP). Основні загрози включають кіберзагрози, тероризм, злочинні дії, природні небезпеки та техногенні аварії.

Німеччина. У Німеччині загрози для критичної інфраструктури чітко класифіковані та включають природні явища, людські прорахунки та технічні збої, а також загрози від тероризму і злочинних дій. Серед природних явищ виділяються паводки, повені, сніг, лід, посухи, урагани, землетруси, пожежі, штормові явища, лавини та зсуви. Загрози від людських прорахунків і технічних збоїв охоплюють технічні збої, помилки в поведінці людей, а терористичні загрози включають злочинні дії, спрямовані на порушення функціонування критичної інфраструктури.

Франція. У Франції загрози критичній інфраструктурі зосереджені на кіберзагрозах та терористичних загрозах. З метою протидії кіберзлочинності та тероризму діє Генеральний секретаріат із питань оборони та національної безпеки (SGDSN), який аналізує відкриту інформацію та розвіддані у сфері захисту критичної інфраструктури, стежить за недопущенням різних загроз – як внутрішніх, так і зовнішніх.

Великобританія. У Великобританії система захисту критичної інфраструктури орієнтована на загрози у сфері державної безпеки, кібербезпеки, тероризму та надзвичайних ситуацій. Центр по захисту національної інфраструктури (CPNI) консультує з питань безпеки підприємства та організації, що є операторами критичної інфраструктури, допомагаючи знизити вразливість національної критичної інфраструктури від тероризму та інших загроз. Національний центр кібербезпеки (NCSC) відповідає за протидію кіберзагрозам, а Секретаріат з питань надзвичайних ситуацій (CCS) сприяє діяльності Центру управління кризовими ситуаціями (COBR), який забезпечує швидке вироблення єдиної позиції та вжиття скоординованих заходів протидії загрозам.

Данія. Данія серед основних загроз для критичної інфраструктури виділяє надзвичайні ситуації, такі як аварії, катастрофи та стихійні лиха. Данське агентство з управління надзвичайними ситуаціями (DEMA) відповідає за збереження та продовження важливих функцій держави та суспільства у разі аварій та катастроф.

Нідерланди. У Нідерландах основні загрози для критичної інфраструктури визначаються через національну оцінку ризиків і включають тероризм, кіберзагрози, забезпечення національної безпеки та кризове управління. Національний координаційний центр із питань боротьби з тероризмом та забезпечення безпеки (NCTV) відповідає за координацію діяльності поліції, судової влади, служб безпеки та інших організацій у сфері боротьби з тероризмом.

Румунія. Румунія поділяє загрози для критичної інфраструктури на такі, що можуть мати природний, випадковий або умисний характер. Природні загрози охоплюють стихійні лиха, випад-

кові загрози включають техногенні аварії, а умисні загрози включають терористичні акти та злочинні дії [9; 11].

Таким чином, загрози критичній інфраструктурі в різних країнах мають спільні риси, проте їх конкретні переліки та класифікації відрізняються залежно від національних пріоритетів і безпекової ситуації. Кожна країна адаптує свої стратегії захисту критичної інфраструктури відповідно до власних потреб і контексту.

Вітчизняний досвід

В Україні немає єдиного підходу до класифікації загроз критичній інфраструктурі. В Концепції створення державної системи захисту критичної інфраструктури, схваленої Розпорядження КМУ від 06.12.2017 р. № 1009-р. визначено загрози для критичної інфраструктури природного та техногенного характеру, протиправні дії та їх комбінації [12]. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII визначає «кіберзагрози» як окремий вид загрози критичній інфраструктурі [13]. В Стратегії кібербезпеки України, затвердженій Указом Президента України від 26.08.2021 р. № 447/2021, серед загроз кібербезпеці виділяють агресію Російської Федерації проти України у кіберпросторі, кіберзлочинність, організовані та спонсоровані урядами інших держав кібератаки, використання кіберпростору терористичними організаціями [14].

У своєму дослідженні О.М. Суходоля визначає ключові загрози для критичної інфраструктури, такі як надзвичайні ситуації (стихійні лиха та техногенні аварії), теракти, диверсії та кіберзагрози [15]. Подібним чином Д.Г. Бобро виділяє техногенні аварії та технічні збої, часто спричинені людськими помилками, стихійними лихами та зловмисними діями як основні загрози критичній інфраструктурі [8].

В свою чергу автори «Зеленої книги» Д.С. Бірюков, С.І. Кондратов, О.І. Насвіт та О.М. Суходоля обґрунтовують ймовірність загроз критичній інфраструктурі через аварії та технічні збої, небезпечні природні явища та зловмисні дії [9].

Для оцінки та порівняння запропонованих класифікацій загроз важливо розглянути принципи, на яких базуються ці класифікації, а також оцінити їх ефективність.

Принципи побудови класифікацій загроз:

Системність та комплексність. Більшість класифікацій загроз побудовані на основі системного підходу, що враховує всі можливі аспекти впливу на критичну інфраструктуру, включаючи природні, техногенні, людські та кіберзагрози. Наприклад, дослідження О.М. Суходолі охоплює широкий спектр загроз, від стихійних лих до кіберзагроз, що дозволяє краще зрозуміти взаємозв'язок між різними типами загроз.

Аналіз причинно-наслідкових зв'язків. У класифікаціях часто враховується зв'язок між різними видами загроз. Наприклад, в роботах Д.Г. Бобра підкреслюється взаємозалежність між техногенними аваріями та людськими помилками, що є ключовим аспектом для запобігання подібних інцидентів.

Акцент на сучасних викликах. Окремі класифікації фокусуються на сучасних загрозах, таких як кіберзагрози, що відображають реалії нових викликів у глобальному інформаційному просторі. Закон України «Про основні засади забезпечення кібербезпеки України» та Стратегія кібербезпеки України є прикладами класифікації загроз, що враховують специфіку кіберпростору.

Адаптивність та актуальність. Класифікації повинні бути адаптивними до змін у геополітичній ситуації та технологічному прогресі. Наприклад, акцент на агресію Російської Федерації у кіберпросторі в Стратегії кібербезпеки України підкреслює важливість врахування загроз.

Запропоновані класифікації загроз критичній інфраструктурі є ефективними у кількох аспектах:

- ***широке охоплення загроз.*** Більшість класифікацій забезпечують комплексний підхід до ідентифікації загроз, що дозволяє вчасно вжити заходів для їх нейтралізації;
- ***фокус на специфічних загрозах.*** Наприклад, виділення кіберзагроз як окремого типу загроз у законодавчих актах України дозволяє зосередити зусилля на захисті критичних інформаційних систем, що особливо важливо у сучасному цифровому середовищі;
- ***здатність реагувати на нові виклики.*** Здатність реагувати на нові виклики, як-от кіберзагрози чи геополітичні ризики, підвищує їхню ефективність у реальному застосуванні.

Беручи до уваги як зарубіжний, так і національний досвід, доцільно сформулювати власну класифікацію загроз критичній інфраструктурі, в яку закладені принципи системності та комплексності, аналізу причинно-наслідкових зав'язків, адаптивності та актуальності.

1. Загрози національній безпеці та обороні:

- терористичні атаки, спрямовані на об'єкти критичної інфраструктури з метою підриву національної безпеки та дестабілізації ситуації в країні;
- диверсії та саботаж, які передбачають дії, спрямовані на пошкодження або знищення об'єктів критичної інфраструктури, що мають стратегічне значення для обороноздатності держави.

2. Кібератаки:

- хакерські втручання, а саме, атаки на інформаційно-телекомунікаційні системи критичної інфраструктури з метою отримання доступу до конфіденційної інформації або порушення їхньої роботи;
- віруси та шкідливе програмне забезпечення, зокрема, розповсюдження шкідливого програмного забезпечення, яке може порушити роботу критичних систем.

3. Економічні загрози:

- економічні санкції, які передбачають введення обмежувальних заходів, що можуть негативно вплинути на функціонування критичної інфраструктури;
- фінансові злочини, такі як шахрайство, відмивання грошей, що можуть підірвати економічну стабільність та фінансову безпеку.

4. Природні та техногенні загрози:

- стихійні лиха, такі як землетруси, повені, урагани, що можуть спричинити руйнування об'єктів критичної інфраструктури;
- техногенні аварії, а саме, аварії на виробництві, технічні збої, які можуть призвести до відмови критичних систем;
- загрози навколишньому середовищу в результаті воєнних дій, зокрема, екологічна шкода (забруднення повітря, води та ґрунту внаслідок використання зброї, руйнування промислових об'єктів та інфраструктури), що може мати довгострокові наслідки для здоров'я населення та екосистем.

Запропонована класифікація загроз критичній інфраструктурі ґрунтується на комплексному аналізі сучасних викликів, з якими стикається Україна, включаючи кіберзагрози, терористичні атаки, економічні санкції, природні катастрофи та техногенні аварії. Вона систематизує загрози за ступенем їхньої небезпеки та потенційного впливу на державу, суспільство та економіку, що дозволяє планувати заходи протидії і захисту з урахуванням специфіки кожного виду загроз.

Ефективність цієї класифікації полягає в її здатності забезпечити всеосяжний підхід до аналізу загроз, який охоплює як традиційні, так і нові виклики. Це досягається завдяки інтеграції принципів системності, комплексності, аналізу причинно-наслідкових зв'язків, адаптивності та актуальності. Такий підхід дозволяє не лише враховувати всі можливі аспекти впливу на критичну інфраструктуру, але й ефективно розподіляти ресурси для їх нейтралізації.

Наукова цінність цієї пропозиції полягає в її здатності інтегрувати різні аспекти загроз у єдину класифікацію, що враховує як внутрішні, так і зовнішні фактори. Це сприяє розробці більш точних і дієвих стратегій захисту критичної інфраструктури, які відповідають сучасним реаліям та специфічним потребам України. Таким чином, класифікація не лише систематизує загрози, але й забезпечує основу для розробки інтегрованих рішень, що підвищують стійкість критичної інфраструктури до різних типів загроз.

Висновки. Класифікація загроз критичній інфраструктурі України, розроблена з урахуванням міжнародного та вітчизняного досвіду, має важливе значення для підвищення рівня національної безпеки. Її користь полягає у систематизації теоретичних знань та поглибленому аналізі сучасних загроз, з якими стикається держава.

Зважаючи на виклики, пов'язані з триваючою війною, зростанням кіберзлочинності та глобальними економічними змінами, запропонована класифікація дозволяє більш чітко потенційні загрози та розробити ефективні стратегії протидії їм. Вона враховує специфіку українського контексту, що робить її особливо корисною для практичного застосування в умовах, що швидко змінюються. Крім того, запропонована класифікація сприятиме всебічному розумінню різних аспектів загроз та забезпечить основу для інтегрованого підходу до їх нейтралізації.

Здобутки дослідження планується використані для подальших наукових пошуків автора, спрямованих на підвищення ефективності організаційних засад протидії кримінальним правопорушенням на об'єктах критичної інфраструктури України в сучасних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ботнаренко І.А. Критична інфраструктура в Україні та її складові: поняття, зміст та законодавче визначення: матеріали Науково-практичної конференції (Львів, 22 грудня 2023). Львів: ЛьвівДУВС, 2024. 192 с.
2. Про затвердження Кодексу системи передачі: Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг № 309 від 14.03.2018 р. ВРУ.2024. URL: https://zakon.rada.gov.ua/laws/show/v0309874-18#Text (дата звернення: 05.08.2024).
3. Про критичну інфраструктуру: Закон України № 1882-IX від 16 листопада 2021 року. ВРУ. 2024. URL: https://zakon.rada.gov.ua/ laws/show/1882-20#Text (дата звернення: 05.08.2024).
4. Директива Ради 2008/114/ЄС про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту від 8 грудня 2008 року. ВРУ. 2008. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text (дата звернення: 05.08.2024).
5. Верголяс О.О. Реформування системи захисту та підвищення стійкості критичної інфраструктури Україні в розрізі актуальних загроз. Coolyanews.info. 2020. URL: https:// coolyanews.info/reformuvannya-sistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriizii-aktual.html (дата звернення: 10.08.2024).
6. Уряднікова І.В., Заплатинський В.М. Наукові підходи до визначення терміну «критична інфраструктура». *Вісті Донецького гірничого інституту*. 2020. № 2 (47). URL: https://jdmi.donntu.edu.ua/wp-content/ uploads/2021/02/Uriadnikova-JDMI_2_2020.pdf (дата звернення: 30.07.2024).
7. Про національну безпеку України: Закон України № 2469-VIII від 21 червня 2018 року. ВРУ. 2023. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 30.07.2024).
8. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети. Серія: Економіка*. 2015. № 4. С. 83–93.
9. Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М. Зелена книга з питань захисту критичної інфраструктури в Україні. Національний інститут стратегічних досліджень. Київ, 2015. URL: https://cdn.regulation.gov.ua/ 6a/69/2a/fa/regulation.gov.ua_File_188.pdf (дата звернення: 30.07.2024).
10. 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.
11. Єрменчук О.П. Оцінка загроз критичній інфраструктурі як важлива складова частини діяльності із захисту державної безпеки. Національний юридичний журнал: теорія і практика. 2018. С. 50К54. URL: https://ibn.idsi.md/ sites/default/files/imag_file/50-54_4.pdf (дата звернення: 30.07.2024).
12. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету міністрів України № 1009-р від 6 грудня 2017 р. ВРУ. 2017. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 30.07.2024).
13. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 5 жовтня 2017 року. ВРУ. 2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.07.2024).
14. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України № 447/2021 від 21 серпня 2021 р. ВРУ. 2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 30.07.2024).
15. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети. Серія: Політика*. 2016. № 3 (40). С. 65–67.