Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 627.25:355.012(043)
DOI: 10.32447/20784643.30.2024.17

А. П. Гаврись, В. В. Філіппова, Н. Ю. Тур
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
ORCID: https://orcid.org/0000-0003-2527-7906 – А. П. Гаврись
https://orcid.org/0000-0003-0771-1975 – В. В. Філіппова
https://orcid.org/0000-0002-0557-5351 – Н. Ю. Тур
✉ Havrys.AND@gmail.com

ІНФОРМАЦІЙНИЙ АНАЛІЗ СИСТЕМ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ПЕРІОД ДІЇ ВОЄННОГО СТАНУ

Анотація. Основною темою статті є захист об'єктів критичної інфраструктури України в умовах воєнного стану. Робота зосереджена на комплексному аналізі сучасних загроз, зокрема воєнних, техногенних, природних та кібернетичних. Особлива увага приділена питанням модернізації та вдосконалення засобів захисту інфраструктури, яка стала мішенню через свою важливість для економічної та соціальної стабільності. Проблема дослідження обумовлена необхідністю забезпечення надійного функціонування критичної інфраструктури, що стало пріоритетною задачею у світлі безпрецедентного зростання атак та технічної вразливості багатьох об'єктів.

Мета статті полягає у аналізі організаційно-технічних та інших рішень для мінімізації ризиків аварій на життєво важливих об'єктах, таких як енергетичні споруди, під час військових конфліктів.

Методи дослідження. Методи дослідження включають аналіз ризиків на основі даних щодо ураження об'єктів внаслідок ракетно-дронових ударів. Порівняльний аналіз міжнародного та вітчизняного досвіду в захисті об'єктів критичної інфраструктури, особливо з урахуванням досвіду функціонування в період воєнного стану.

Результати дослідження. Автори статті виокремлюють певний комплекс заходів для зміцнення захисту, зокрема впровадження новітніх методів моніторингу та управління ризиками з метою мінімізації збитків від можливих катастроф, що викликані як природними, так і антропогенними факторами, узагальнюють та представляють у вигляді блок-схем ці заходи захисту для об'єктів критичної інфраструктури та енергетичних об'єктів України.

Тому модернізація критичної інфраструктури України та використання новітніх засобів захисту є важливим кроком у зниженні вразливості країни до зовнішніх і внутрішніх загроз. Ці дослідження закладають основу для подальших науково-практичних рішень у сфері захисту критичної інфраструктури, що є національним пріоритетом в умовах сучасних викликів і ризиків.

Ключові слова: об'єкти критичної інфраструктури, гідротехнічні споруди, воєнний стан, техногенні аварії, надзвичайна ситуація.

A. P. Havrys, V. V. Filippova, N. Yu. Tur
Lviv State University of Life Safety, Lviv, Ukraine

INFORMATION ANALYSIS OF CRITICAL INFRASTRUCTURE PROTECTION SYSTEMS DURING MARTIAL LAW

Abstract. The main theme of the article is the protection of Ukraine's critical infrastructure under martial law conditions. The work focuses on a comprehensive analysis of current threats, including military, technological, natural, and cyber threats. Special attention is given to the modernization and improvement of protective measures for infrastructure, which has become a target due to its significance for economic and social stability. This study addresses the urgent need to ensure the reliable operation of critical infrastructure, which has become a priority due to the unprecedented increase in attacks and the technical vulnerability of many facilities.

The article aims to analyze organizational, technical, and other solutions to minimize the risk of accidents at vital facilities, such as energy installations, during armed conflicts.

Research methods. The research methods include risk analysis based on data on infrastructure damage from missile and drone strikes. A comparative analysis of international and domestic experiences in critical infrastructure protection, especially considering operations under martial law, was also conducted.

Research results. The authors outline a set of measures to strengthen protection, including the implementation of modern monitoring and risk management techniques to minimize the damage from potential disasters caused by both

natural and anthropogenic factors. These protective measures for critical infrastructure and energy facilities in Ukraine are summarized and presented in the form of block diagrams.

Therefore, modernizing Ukraine's critical infrastructure and employing the latest protective measures are essential steps in reducing the country's vulnerability to external and internal threats. This research establishes a background for further scientific and practical solutions in the field of critical infrastructure protection, which is a national priority amid modern challenges and risks.

Key words: objects of critical infrastructure, hydrotechnical structures, martial law, man-made accidents, emergency situation

Вступ. Одне з найактуальніших питань сучасності – як захистити об'єкти критичної інфраструктури від надзвичайних ситуацій природного, техногенного, соціального характеру, а також під час військових конфліктів. Об'єкти критичної інфраструктури стають легкою мішенню для ворога і порушення функціонування одного об'єкта може призвести до так званого «ефекту доміно», тобто впливати на інші об'єкти, що призводить до створення проблем нормального їх функціонування та порушення життєдіяльності населення країни.

Проблематика дослідження полягає в ідентифікації та розв'язанні ключових викликів, пов'язаних із безпекою та стійкістю критично важливих об'єктів, які включають зростаючі загрози фізичної безпеки, оскільки в умовах воєнного стану підвищуються ризики прямих атак на об'єкти критичної інфраструктури, таких як ракетні обстріли, диверсії та інші акти вандалізму; кіберзагрози, зокрема хакерські атаки, що стають серйозною проблемою для критичної інфраструктури, яка все більше залежить від автоматизованих систем управління та передачі даних; недостатню координацію та управлінські складнощі, оскільки захист критичної інфраструктури потребує комплексного підходу, що включає координацію між військовими, урядовими структурами, правоохоронними органами, місцевою владою і приватними операторами інфраструктури; обмежені фінансові і матеріальні ресурси, адже захист об'єктів потребує значних ресурсів для впровадження певних заходів; зношеність обладнання на об'єктах, стійкість та підготовка персоналу, оскільки такі співробітники потребують спеціальних навичок до дій у надзвичайних ситуаціях.

Методи дослідження. Аналіз ризиків спрямований на визначення виду об'єктів ураження ракетно-дроновими атаками та їх кількості, а також на виявлення можливих наслідків цих подій. Методика аналізу включає вивчення актуальних зовнішніх загроз, таких як військові дії чи природні катастрофи. Цей метод дає змогу оцінити рівень небезпеки для об'єктів та виробити стратегію зменшення ризиків, що сприятиме підвищенню безпеки таких об'єктів.

Для вивчення зарубіжного досвіду у питанні захисту об'єктів критичної інфраструктури використовувався порівняльний аналіз. Досвід інших країн, які стикаються з певними проблемами в захисті об'єктів критичної інфраструктури та знаходять рішення щодо вирішення цих проблем показує нам, які ефективні стратегії захисту можна адаптувати до ситуації, в якій перебуває наша країна.

У рамках дослідження використовувався також системний аналіз, який дає змогу розглянути критичну інфраструктуру як комплексну систему, де кожен об'єкт є взаємопов'язаною ланкою. Системний аналіз дозволяє передбачити можливі наслідки для всієї системи у разі пошкодження одного або декількох ключових об'єктів, тим самим сприяючи розробці більш цілісних стратегій захисту.

Результати дослідження. Оскільки здатність держави підтримувати важливу діяльність суспільства під час кризи, особливо під час стихійних лих, техногенних аварій, кібератак чи військових конфліктів, залежить від функціонування критичної інфраструктури, її захист став одним із найважливіших завдань у XXI столітті. В сучасному середовищі, де гібридні загрози стають все більш частими, захист об'єктів критичної інфраструктури потребує ретельної стратегії, яка враховує як кібернетичні, так і фізичні загрози.

В країнах, де існує загроза чи триває збройний конфлікт, захист життєво важливої інфраструктури є пріоритетним завданням. Стратегічне значення секторів критичної інфраструктури, таких як: паливно-енергетичний, фінансовий, інформаційний, цифрових технологій, захисту інформації, харчової промисловості та агропромислового комплексу, державного матеріального резерву, охорони здоров'я, ринків капіталу та організованих товарних ринків, транспорту і пошти, системи життєзабезпечення, промисловості, громадської безпеки, цивільного захисту населення і територій, охорони навколишнього природного середовища, оборони, правосуддя, виконання кримінальних покарань, тримання під вартою та утримання військовополонених, державної реєстрації, наукових досліджень та розробок, виборів та референдумів, соціального захисту, державної

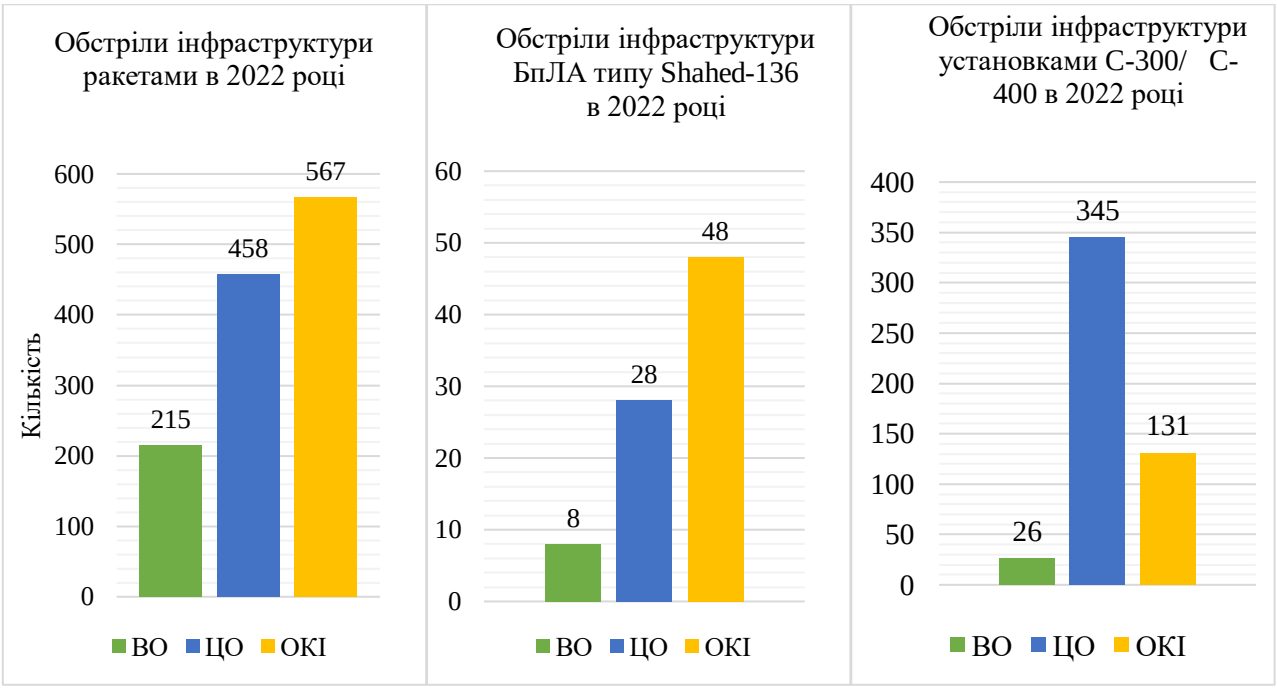
влади та місцевого самоврядування, що використовуються для основних операцій і оборонних можливостей держави, робить об'єкти критичної інфраструктури значно вразливими під час війни. Атаки на такі об'єкти можуть серйозно послабити обороноздатність країни, та призвести до порушення систем життєзабезпечення населення. Як наслідок, в контексті сучасних загроз і конфліктів об'єкти критичної інфраструктури перетворюються на основну ціль ворога.

Зокрема з 2014 року на східній території нашої країни почалася антитерористична операція. В 2022 році ця операція переросла в повномасштабні військові дії, в яких частина наших областей була захоплена ворогом. Певну територію вдалося звільнити, але більшість окупованої території перебуває під владою терористів. В той же час, вся територія України піддається щоденним обстрілам з різної зброї. Ракети, безпілотні літальні апарати, КАБи, авіабомби, балістика, все це тягне за собою матеріальні, культурні, природні, екологічні, фінансові збитки, але одне з найбільших лих, що спричиняє війна, це те, що вона забирає людські життя і не тільки на полі бою, а й в містах, які віддалені від лінії фронту, завдаючи обстрілів, по приватних секторах, багатоквартирних будинках, школах, лікарнях, приватних установах, пожежних частинах, пансіонатах, дитячих будинках, підприємствам державної та приватної власності та вкрай важливих об'єктах життєзабезпечення населення.

Аналіз обстрілів є важливим для розуміння масштабів та тенденцій атак, з якими стикнулася Україна з початку 2022 року. Згідно із статистичними даними [1], засобами масової інформації та Інтернет-ресурсами вдалося визначити кількість обстрілів та потенційні об'єкти ураження. Представлені статистичні дані мають на меті ознайомити та допомогти у плануванні відповідних заходів для підвищення безпеки об'єктів.

На рисунку 1 висвітлено кількість обстрілів ракетами (рис. 1а), БпЛА типу Shahed-136 (рис. 1б) та установками С-300/С-400 (рис. 1в), завданих по військових об'єктах, цивільних об'єктах та об'єктах критичної інфраструктури від початку повномасштабного вторгнення до кінця 2022 року. Як бачимо з рисунка 1а та 1б в перший рік повномасштабного вторгнення, ураження об'єктів, спричинені ракетами значно переважають ураження від Shahed-136, оскільки перший Shahed-136, який був зафіксований та збитий у Харківській області 12 вересня 2022 року, після того як ворог отримав їх від своїх союзників у бойове використання.

На рисунку 1в висвітлено дані щодо ураження об'єктів інфраструктури з зенітно-ракетних комплексів середнього радіуса дії. 18 червня 2022 року агресор вперше обстріляв територію України з комплексу С-300.



а б в

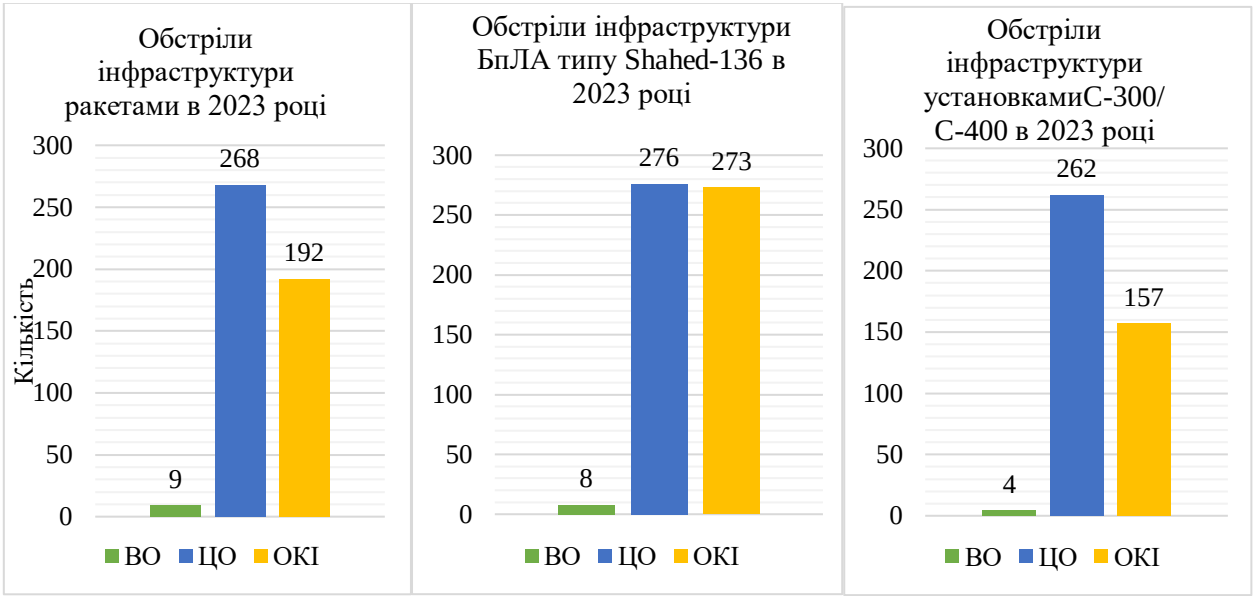
Рисунок 1 – Обстріли інфраструктури України в 2022 році відповідно до даних з [1]

На другому році війни окупанти зосередились на обстрілах цивільної інфраструктури. Як бачимо, на рисунку 2 висвітлено дані щодо ураження об'єктів інфраструктури України в 2023 році, де можна помітити значну перевагу обстрілів цивільної інфраструктури над військовою та дещо більшою

ніж ураження об'єктів критичної інфраструктури. На рисунку 2а в порівнянні з попереднім роком кількість ураження об'єктів ракетами зменшилась, але на рисунку 2б чітко проглядається зростання ударів по об'єктах Shahed-136.

На рисунку 2в в порівнянні з попереднім роком зменшилась кількість ураження об'єктів інфраструктури з установок С-300/С-400. Це пов'язано із збільшенням використанні БпЛА типу Shahed-136.

Варто зазначити, що статистика по об'єктах військової інфраструктури значно зменшилась, але це не означає, що і зменшилась кількість обстрілів військової інфраструктури. Дані щодо ураження такої інфраструктури не завжди висвітлюють в ЗМІ, з безпекових міркувань.



а б в

Рисунок 2 – Обстріли інфраструктури України в 2023 році відповідно до даних з [1]

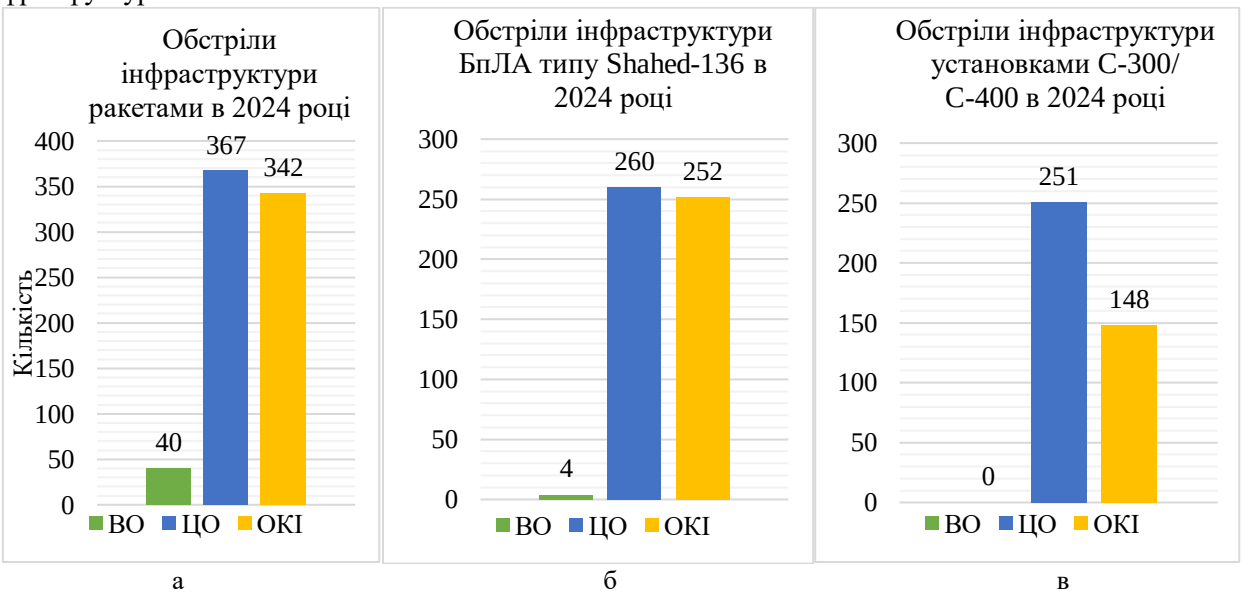
В 2024 році кількість обстрілів країни не зменшилась. Ворог активно застосовує нові види зброї та завдає ударів по інфраструктурі країни.

З рисунка 3, бачимо що ворог активізував використання ракет для завдання ударів та продовжує застосовувати Shahed-136 і С-300/С-400.

Обстріли цивільної інфраструктури знову залишаються на першому місці, як і в минулому році в порівнянні з критичною та військовою інфраструктурою.

На рисунку 3а помітно збільшилась кількість уражень об'єктів критичної інфраструктури та незначно виросла статистика обстрілів військових об'єктів в порівнянні з минулим роком.

Дані з рисунка 3б та 3в такі ж як і минулорічні щодо ураження цивільних об'єктів та об'єктів критичної інфраструктури. Дані про обстріли військових об'єктів з С-300/С-400 не були представлені в ЗМІ та інтернет-просторах.



а б в

Рисунок 3 – Обстріли інфраструктури України в 2024 році відповідно до даних з [1]

Аналізуючи статистику обстрілів інфраструктури України та озброєння, з якого уражають об'єкти з настанням 2024 року збільшилась кількість використання авіабомбових ударів. Оскільки інформація щодо місць скидання, кількості та наслідків ударів, є неточною, ця інформація тут не висвітлена. Однак, кількість атак з такого озброєння постійно збільшується на північно-східній, східній та південно-східній території України.

Підсумовуючи вищенаведену статистику з рисунків за період повномасштабного вторгнення, ворог завдав як мінімум 314 ударів по військових об'єктах, приблизно 2515 – по цивільних та уразив щонайменше 2110 об'єктів критичної інфраструктури.

З аналізу ударів по інфраструктурі України бачимо, що значній атаці підпадають об'єкти критичної інфраструктури. Згідно з [2], до переліку секторів критичної інфраструктури входить і паливно-енергетичний комплекс, що включає електроенергетику. Енергетична інфраструктура забезпечує роботу практично всіх інших галузей — від транспорту і зв'язку до медицини та житлово-комунальних послуг. Зруйнування або порушення роботи об'єктів електроенергетики спричиняє серйозні перебої в життєдіяльності населення, що робить енергетичну систему однією з головних мішеней для ворога.

Зі статистичних даних, наведених на рисунку 4, проаналізувавши обстріли об'єктів критичної інфраструктури за час повномасштабного вторгнення, бачимо, що ворог завдає ударів по об'єктах енергетики з початку війни.

У 2022 році були уражені 193 об'єкти енергетики з 746 об'єктів критичної інфраструктури, у 2023 році - 65 об'єктів із 622, а в 2024 - 167 об'єктів із 742.

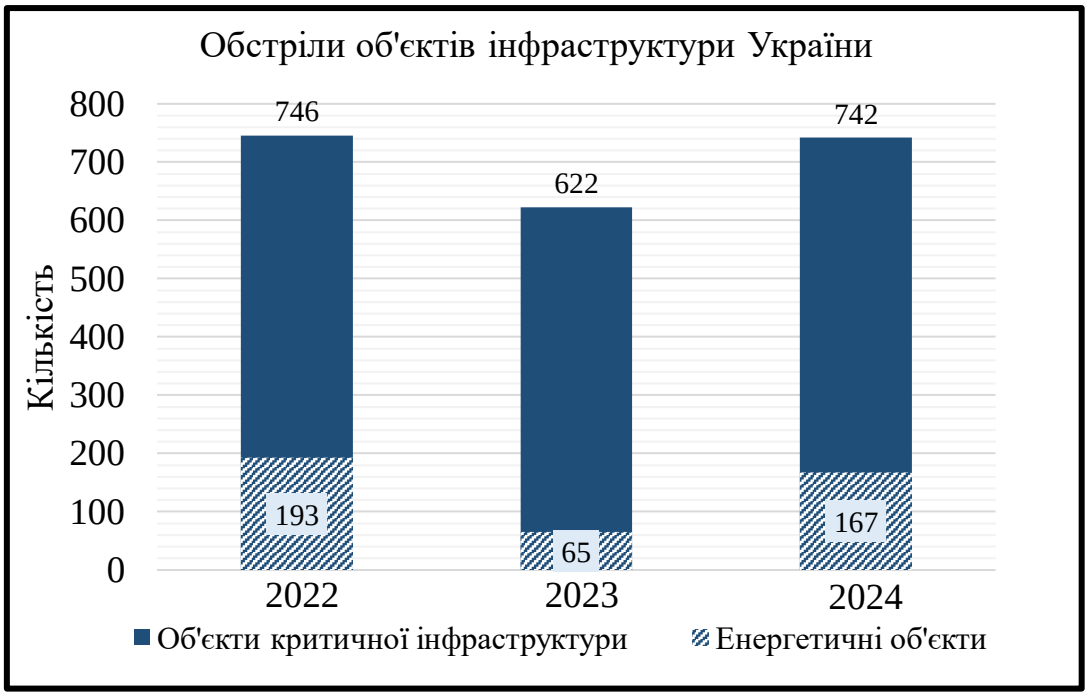


Рисунок 4 – Обстріли критичної та енергетичної інфраструктури України під час повномасштабного вторгнення, відповідно до даних з [1]

Такі атаки призводять до знеструмлення цілих регіонів, дестабілізуючи населення країни та створюючи проблеми в життєво необхідних комунікацій, таких як світло, тепло та водопостачання, насамперед, в період похолодання. Варто зазначити, що енергетична інфраструктура для нашої держави є ключовою для забезпечення більшості вагомих сфер економіки держави та експорту електроенергії закордон.

Тому, створення умов для нормального функціонування об'єктів енергетики в час повномасштабного вторгнення потребує дослідження та пошуку рішень для їх захисту.

Аналізуючи наукові джерела для розуміння досвіду захисту об'єктів критичної інфраструктури в зарубіжних країнах бачимо, що питання захисту таких об'єктів для кожної країни є основним через значну залежність населення та держави загалом від них.

Автори статті [3] розглядали зростаючу загрозу кібератак на критичну інфраструктуру та представили порівняльну структуру для оцінки кіберврразливості основних секторів на основі таких факторів, як впровадження нових технологій, наявність застарілих систем, матеріальні наслідки та наслідки щодо безпеки зламів, а також цінність скомпрометованих

даних. Автори надали стратегічні рекомендації для державних і приватних зацікавлених сторін щодо співпраці між секторами для вдосконалення стандартів, обміну інформацією, досліджень і розробок та розвитку робочої сили.

У статті [4] розглядається стійкість критичної інфраструктури з точки зору того, як її можна включити в існуючі практики безпеки, а саме стандарт управління ризиками ISO 31000. Автори запропонували розширення стандарту управління ризиками до основи управління стійкістю критичної інфраструктури. Зосереджуючись, зокрема, на сферах організаційної та технологічної стійкості, які вважаються такими, якими найпростіше керувати операторам критичної інфраструктури У статті детально представлений один із методів оцінки стійкості для введення в дію загальної структури управління.

У статті [5] досліджуються вразливості та загрози, з якими стикаються сучасні критичні інфраструктури, з особливим наголосом на промислових системах керування, а також описується ряд заходів захисту. Також обговорюються деякі складні сфери, пов'язані із захистом критичної інфраструктури, такі як управління безпекою, захищені мережеві архітектури, самовідновлення, моделювання та симуляція, ситуаційна обізнаність у широкій зоні, а також управління довірою та конфіденційність.

Автори статті [6] проаналізували державну політику щодо розвитку законодавства про критичну інфраструктуру в Європейському Союзі, що охоплює 27 розвинених країн. Дійшли висновку, що нормативно-правові документи свідчать про посилення регулювання сектору критичної інфраструктури, як розширюючи так і поглиблюючи наднаціональні тенденції в цій сфері. Запропонували стандартизацію певного базового рівня оцінки стійкості КІ.

Автори статей [7, 8] описали теоретичні засади функціонування об'єктів критичної інфраструктури, де увагу зосередили на критичному аналізі трактування визначень об'єктів критичної інфраструктури та безпеки об'єктів, вказали на обставини, за яких необхідно організовувати безпеку таких об'єктів та обґрунтували потребу в формуванні єдиної державної політики щодо захисту об'єктів критичної інфраструктури в Україні.

У своїй роботі автори статей [9 - 12] досліджували спектр загроз для об'єктів критичної інфраструктури і розглядали вітчизняний та зарубіжний досвід щодо захисту таких об'єктів. На основі опрацьованих даних, автори, науково обґрунтували основи забезпечення національної системи захисту об'єктів критичної інфраструктури країни та дійшли до низки висновків стосовно внесення змін до нормативно-правових документів щодо захисту такої інфраструктури в Україні. А в статті [13] автор визначив види загроз для критичної інфраструктури України в умовах військового стану та на основі аналізу вітчизняного і зарубіжного досвіду сформулював власну класифікацію загроз для об'єктів критичної інфраструктури в державі.

Автори [14, 15] розглядали питання управління ризиками об'єктів критичної інфраструктури і запропонували власну інтерпретацію трактування поняття «ризик функціонування об'єктів критичної інфраструктури» яка ґрунтується на аналізі, синтезі та теоретичному узагальненні, а також визначили ключову специфіку ризиків на таких об'єктах і ризик-менеджмент їх функціонування. У статті подано рекомендації заходів щодо покращення внутрішнього стану захисту критичної інфраструктури.

Автор [16] висвітлює проблеми захисту критичної інфраструктури України та необхідність організації протидії цим загрозам. Результатом статті є створення сучасної моделі загроз, яка формалізує ймовірні впливи на критичну інфраструктуру, що дасть змогу підвищити ефективність її захисту.

У статті [17] запропоновано структурно-лінгвістичну схему методології побудови системи захисту та безпеки об'єктів критичної інфраструктури з позицій зниження результативності ризиків. Виконали аналіз системи оцінювання ризику безпеки сукупності ОКІ та доступу до неї і обґрунтували доцільність підвищених зобов`язань щодо метрологічної надійності засобів вимірювання з метою виконання жорстких вимог з оцінки ризиків кібербезпеки в умовах реалізації принципу невизначеності при забезпеченні достовірності вимірювань.

Країни світу з розвиненою критичною інфраструктурою активно зміцнюють свою оборону, створюючи всеохоплюючі національні стратегії захисту критичної інфраструктури. Ці тактики включають встановлення державно-приватного партнерства, впровадження передових технологій, таких як штучний інтелект та машинне навчання, сприяння глобальній співпраці у сфері кібербезпеки та обмін інформацією про загрози. Також варто зазначити, щоб посилити захист і стійкість критичної інфраструктури, важливо, щоб персонал, який її обслуговує, був обізнаний у своїй діяльності. Авторами статті [18] проведено аналіз нормативно-правової бази підготовки фахівців у сфері захисту критичної інфраструктури, узагальнено освітню практику захисту таких об'єктів у провідних країнах світу та запропоновано

механізм запровадження системи навчання фахівців у сфері захисту критичної інфраструктури. Також авторами статті [19] проведено аналіз теоретико-методологічних засад підготовки фахівців з реагування на кризові ситуації на об'єктах критичної інфраструктури Україні та надано практичні рекомендації щодо системи підготовки та підвищення кваліфікації персоналу у сфері захисту критичної інфраструктури щодо розвитку державно-приватного партнерства, а також проведення міжвідомчих командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять.

Управління інформаційною безпекою на об'єктах критичної інфраструктури є важливим чинником забезпечення безпеки на такому об'єкті, авторами статті [20] досліджено системи управління інформаційною безпекою як інструментом підвищення рівня захисту та ефективності об'єктів критичної інфраструктури та проведено порівняльний аналіз аналогічних рішень, який визначив найбільш оптимальні методи та підходи до управління інформаційною безпекою, які сприятимуть збільшенню рівня захисту об'єктів критичної інфраструктури.

Огляд літератури, присвячений організаційним рішенням у сфері захисту критичної інфраструктури, висвітлив важливість ефективної координації між різними державними та приватними структурами, впровадження стратегічних підходів до управління ризиками та розробки планів реагування на надзвичайні ситуації. Однак, для забезпечення комплексного захисту необхідно враховувати також технічні аспекти.

У статті [21] автори досліджують використання технології блокчейн для вирішення проблем захисту критичної інфраструктури, підкреслюючи її незмінність, децентралізацію та прозорість як ключі до посилення стійкості цих життєво важливих структур. Ця робота демонструє потенціал блокчейна для посилення критичної інфраструктури. Це знаменує прогрес у практичному застосуванні блокчейну, пропонуючи чіткий напрямок майбутніх досліджень і розробок у цій галузі, що розвивається.

Загрозою для об'єктів критичної інфраструктури є також стихійні лиха, такі як вулкани, землетруси, торнадо та урагани, паводкові затоплення, тому автори статті [22, 23] у своїй роботі представляють аналітичну модель для кількісної оцінки потенційної шкоди електростанціям від землетрусу та економічної оцінки ефективності заходів для підвищення їх сейсмостійкості.

Статті [24, 25] присвячені удосконаленню науково-методичного апарату обчислення ризиків виникнення та аналізу сценаріїв надзвичайних ситуацій на об'єктах критичної інфраструктури. Автори розробили моделі для прогнозування та мінімізації впливу надзвичайних ситуацій з метою запобігання руйнівним наслідкам.

Автори статті [26] описують науково-методичний підхід до оцінки безпеки критичної інфраструктури з використанням комплексів захисту від безпілотних літальних апаратів та крилатих ракет. Автори аналізують сучасні методи протидії, висвітлюють проблеми виявлення і супроводження малорозмірних цілей через їх особливі характеристики, що ускладнюють ефективність захисних заходів. Автори пропонують поділ системи оборони на інформаційну, керуючу, виконавчу та забезпечувальну підсистеми, кожна з яких оцінюється за конкретними критеріями. Це дасть змогу визначати загальну ефективність захисту та оптимізувати витрати на основі співвідношення ефективність-вартість.

У статті [27] автори аналізують методи моделювання безпеки у відповідь на терористичні загрози, розділяючи заходи на три основні групи: засоби виявлення загрози, знищення загрози, та ліквідація наслідків. Робота підкреслює значення статистичної ймовірності як ключового показника для оцінки ефективності захисних заходів.

Автор [28] у своїй роботі досліджував інженерно-технічні методи запобігання надзвичайним ситуаціям техногенного характеру на об'єктах критичної інфраструктури за допомогою оперативного стану контролю повітряного середовища в приміщеннях та на прилеглій території об'єктів. На основі проведеного дослідження розробив нові науково-обґрунтовані математичні моделі та відповідні інженерно-технічні методи запобігання таким ситуаціям техногенного характеру на об'єктах критичної інфраструктури за допомогою оперативного стану контролю повітряного середовища.

Автори статті [29] розглядають практики та заходи, що використовуються на державному рівні для забезпечення кібербезпеки критичної інфраструктури та висвітлюють шляхи зміцнення державних підходів і механізмів досягнення стратегічних цілей щодо захисту інфраструктури. В статті наголошується на необхідності комплексного підходу в управлінні кібербезпекою критичної інфраструктури для зменшення вразливості критично важливих об'єктів, пом'якшення потенційних наслідків кіберінцидентів або несприятливих подій на таких об'єктах; а також для ідентифікування, стримування, виявлення, попередження та готовності до кіберзагроз і небезпек на критичній інфраструктурі України.

Автори [30] провели огляд досліджень щодо прийняття рішень з точки зору ризик-

інформаційної безпеки комплексу об’єктів критичної інфраструктури та проаналізувавши методологічну побудову структурно-лінгвістичної схеми вибору засобів захисту комплексу об’єктів критичної інфраструктури з точки зору зниження ризику і на прикладі виявлення несанкціонованих атак зловмисників за допомогою дронів та радіофізичних систем, як засобів вимірювання навколишнього середовища у вигляді схемотехнічної реалізації кореляційного радара, показали доцільність і можливість виявлення потенційної атаки зловмисника.

Автори статті у своєму дослідженні [31] за допомогою системного аналізу, розробили стратегію визначення оптимальних місць розміщення засобів фізичного впливу та використовуючи математичне моделювання, оцінювали ефективність взаємодії засобів фізичного радіоелектронного впливу в контексті захисту об’єктів критичної інфраструктури енергетичного комплексу від авіаударів.

Автор статті [32] вивчає ураження об’єктів критичної інфраструктури ракетними ударами противника. Він детально описує основні види зброї, які використовуються для атак на українські об’єкти, а також методично пояснює розрахунок захисної товщини підземних укриттів для цих об’єктів, опираючись на аналіз головних компонентів інфраструктурних об’єктів в енергетичному секторі, показав доцільність створення такого укриття.

В статті [33] автори розробили методику розрахунків та обґрунтували вимоги до елементів інженерного захисту об’єктів критичної інфраструктури електроенергетичної та газотранспортної систем України від БпЛА типу «Shahed-136». Також розглянули характеристики та конструкцію цієї зброї. Обґрунтували вимоги до облаштування та запропонували принципове рішення першочергового кільцевого інженерного захисту найважливіших споруд та обладнання таких об’єктів. А в статті [34] автори розглядають деякі аспекти класифікації безпілотних літальних апаратів на користь захисту об’єктів критичної інфраструктури. Автори проаналізувавши поняття класифікація, її види та призначення і охарактеризувавши деякі існуючі системи класифікації БпЛА, запропонували варіант класифікації на користь захисту таких об’єктів.

У статті [35] авторами досліджуються шляхи підвищення ефективності систем фізичного захисту об’єктів критичної інфраструктури, які забезпечують запобігання терористичним актам. Описано функціональність систем захисту, що включає сигналізацію, оптоелектронне спостереження, контроль доступу, зв'язок і освітлення. В статті також розглядається управління надзвичайними ситуаціями, включаючи моніторинг та аналіз ризиків. Пропонуються вдосконалення, за допомогою акустичних систем контролю, що можуть підвищити ефективність спостереження на значній відстані та допомагати виявляти потенційні загрози.

Автори статті [36] розглядають як захист існуючих об’єктів, так і проектування нових з урахуванням вимог до інженерного та цивільного захисту. Наведені методи оцінки ризику пошкодження критичної інфраструктури, методи їх інженерно-аналітичних розрахунків та методи інженерно-конструктивного захисту від боєприпасів різних типів дозволяють розробити ефективну комплексну систему захисту стратегічно важливих об’єктів.

У статті [37] автор досліджує питання забезпечення кібербезпеки об’єктів критичної інфраструктури на основі штучного інтелекту в умовах воєнного стану. На підставі аналізу позитивного американського досвіду, запропоновані заходи з удосконалення забезпечення кіберзахисту об’єктів критичної інфраструктури України. Запропоновані рекомендації у сфері інформаційної безпеки, що базується на властивостях інформації та досягненнях інформаційно-комунікаційних технологій і систем.

Для захисту життєво важливих об’єктів інфраструктури необхідно комплексно використовувати технічні та організаційні рішення, які передбачають декілька підходів, зокрема захист від терористичних та диверсійних атак, гарантування інформаційної безпеки, розробку систем раннього виявлення загроз та створення систем резервного копіювання, які дозволяють оперативно відновлювати працездатність інфраструктури у разі нещасних випадків або нападів. В умовах військового стану важливим критерієм захисту критичної інфраструктури є виявлення та знешкодження фізичних загроз, а також укріплення об’єктів, використовуючи певні конструкції.

На рисунку 5 зображено блок-схему заходів із захисту критичної інфраструктури України під час дії військового стану.

Рисунок 5 – Блок схема заходів із захисту об’єктів критичної інфраструктури України

Ця блок-схема ілюструє комплексний підхід до захисту критичної інфраструктури, де поєднуються організаційні заходи та технічні інновації для максимального захисту від можливих загроз. Організаційні заходи спрямовані на забезпечення належної координації, розподілу відповідальності, планування, залучення міжнародного досвіду та підготовки персоналу. Технічні заходи спрямовані на моніторинг, управління ризиками, застосування новітніх технологій, фізичний захист об’єктів, розробку систем раннього виявлення загроз та кібербезпеку [38].

Забезпечення функціонування та захист енергетичної інфраструктури є одним з аспектів безпеки під час воєнного стану. Основні атаки на енергетичну інфраструктуру включають ракетні удари, атаки безпілотних літальних апаратів, кібератаки та інші методи дестабілізації, спрямовані на електростанції, лінії електропередач та інші енергетичні вузли. Такі удари не лише виводять з ладу об’єкти, але й створюють довготривалі наслідки, які позначаються на інших галузях економіки та житті населення.

Тому розробка інтегрованих систем управління ризиками, які об’єднують методи оцінки й моніторингу загроз та створюють можливість для швидкого реагування на них; використання системного аналізу для оцінки впливу пошкоджень одного об’єкта на функціонування всієї інфраструктури; впровадження багаторівневих стратегій безпеки, які включають фізичний захист, захист від кібератак та заходи з відновлення об’єктів у випадку ураження; впровадження автоматизованих систем моніторингу, що дають можливість постійно відстежувати стан об’єктів та виявляти ознаки пошкоджень чи загроз у реальному часі; використання безпілотних літальних апаратів для дистанційного моніторингу, діагностики та огляду об’єктів після атак, що значно скорочує час реакції та підвищує ефективність відновлювальних робіт; застосування інтелектуальних систем управління ризиками, які аналізують дані з численних джерел та надають рекомендації для оперативного прийняття рішень; зміцнення фізичних конструкцій об’єктів енергетичної інфраструктури для підвищення їхньої стійкості до прямих атак, включаючи ракети, дрони та інше озброєння агресора; впровадження сучасних технологій, таких як кіберстійкі системи для захисту від кібератак, що знижують ймовірність виведення з ладу інфраструктури внаслідок хакерських атак та розширене застосування технологій блокчейну для забезпечення надійності передачі та збереження даних, а також для підвищення рівня прозорості та

безпеки операцій з управління інфраструктурою є рішучими діями забезпечення безпеки об’єктів енергетичної інфраструктури і сприяють формуванню комплексного підходу до захисту енергетичної інфраструктури, підвищуючи її стійкість до сучасних загроз і забезпечуючи стабільність роботи навіть в умовах кризи.

На рисунку 6 зображено узагальнені заходи захисту об’єктів енергетичної інфраструктури, які доцільно реалізувати на енергетичних об’єктах України, для зниження ризиків атак, безперебійної роботи об’єктів та оперативне реагування на надзвичайні ситуації.

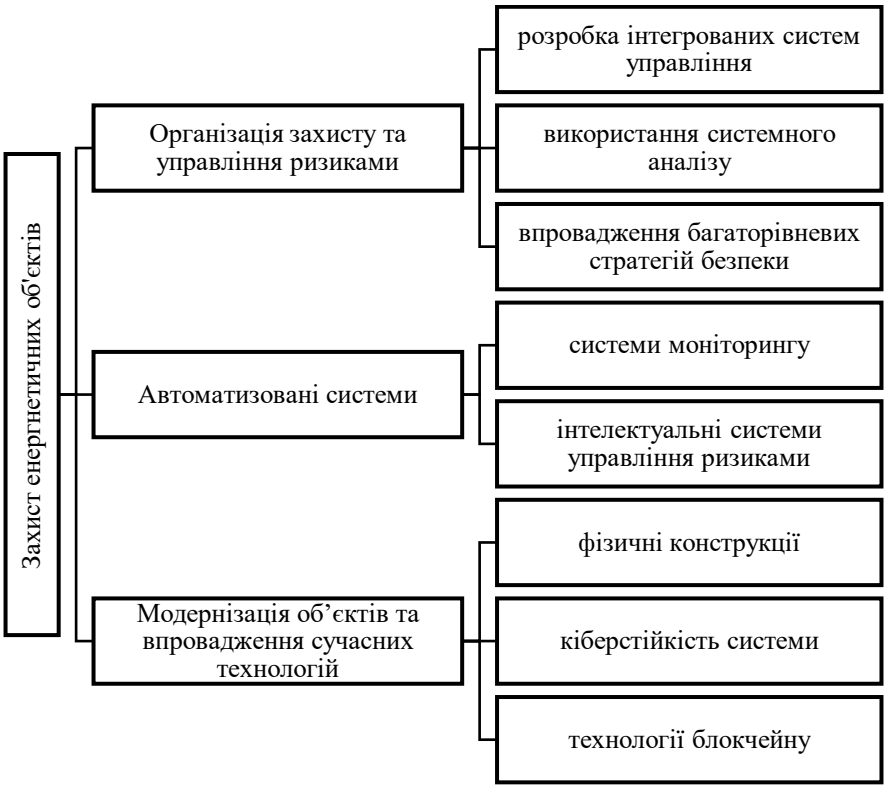


Рисунок 6 – Блок-схема заходів із захисту енергетичної інфраструктури України

Ця блок-схема описує різні аспекти захисту енергетичних об’єктів, та складається з трьох основних напрямків: організація захисту та управління ризиками, автоматизовані системи, модернізація об’єктів та впровадження сучасних технологій.

Організація захисту та управління ризиками передбачає системний підхід до планування та впровадження заходів безпеки на енергетичних об’єктах. Метою напряму є зниження рівня ризиків та забезпечення стійкості об’єктів до різних загроз. Він включає створення єдиних платформ, що дозволяють об’єднувати різні аспекти управління безпекою на одному об’єкті; застосування методик аналізу для оцінки ризиків і виявлення слабких місць в існуючих системах захисту та розробку багатошарової структури захисту, що передбачає кілька рівнів безпеки.

Автоматизація відіграє важливу роль у сучасному захисті енергетичних об’єктів, оскільки дає змогу знижувати вплив людського фактора та забезпечує високу точність у моніторингу і реагуванні. До цієї категорії відносяться автоматизовані системи спостереження та збору даних в режимі реального часу та застосування технологій штучного інтелекту для прогнозування ризиків і оптимізації процесу ухвалення рішень.

Модернізація об’єктів та впровадження сучасних технологій зосереджена на підвищенні фізичної та інформаційної безпеки через інновації та модернізацію існуючих об’єктів та включає: будівництво захисних споруд, зміцнення існуючих конструкцій та інші заходи для підвищення стійкості об’єкта до фізичних загроз; використання сучасних технологій шифрування, аутентифікації та засобів запобігання несанкціонованому доступу та впровадження блокчейн-технологій для підвищення прозорості і захищеності операцій.

Висновки

В статті проаналізовано захист об’єктів критичної інфраструктури України під час військового конфлікту, підкреслюючи складність сучасних загроз і необхідність комплексного підходу.

У роботі чітко підкреслено, що критична інфраструктура є основою життєдіяльності

країни, оскільки забезпечує функціонування економіки, транспорту, зв'язку та комунальних послуг для населення. Модернізація об'єктів інфраструктури, використання систем моніторингу та посилення фізичного захисту значно підвищують стійкість до атак, включаючи ракетні та кібернетичні загрози.

Також авторами доведено, що захист енергетичних об'єктів є пріоритетом, оскільки енергетичний сектор України є стратегічно важливою частиною інфраструктури, а знищення чи пошкодження об'єктів енергетики призводить до знеструмлення великих регіонів, що в свою чергу паралізує роботу підприємств, лікарень, шкіл та інших важливих установ. Ураження цих об'єктів може ускладнити логістику, ремонт техніки, виробництво зброї та інші оборонні процеси. Відсутність електроенергії та тепла в умовах холодної погоди створює серйозні проблеми для здоров'я громадян України.

У підсумку, в умовах безпрецедентного зростання атак та техногенних загроз, запропоновані заходи покликані не лише підвищити стійкість інфраструктури до руйнувань, але й сприяти стабільності держави та безпеці її громадян. Досвід, отриманий з аналізу міжнародних практик, дозволяє Україні адаптувати ефективні стратегії для захисту критичної інфраструктури, а також розробляти національні підходи, що враховують специфіку сучасного конфлікту та необхідність оперативного реагування. Ці висновки та рекомендації можуть слугувати фундаментом для подальших наукових та прикладних досліджень, спрямованих на формування комплексної системи захисту об'єктів критичної інфраструктури у контексті глобальної та національної безпеки.

Список літератури:

1. Статистика повітряних тривог. URL: https://air-alarms.in.ua/?from=2022-02-24&to=2024-08-30#statistic.

2. Постанова Кабінету Міністрів України Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури : прийнята 22 липня 2022 року № 821.

3. Shaji George, A., Baskar, T., & Balaji Srikaanth, P. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. Partners Universal International Innovation Journal (PUIIJ), 02(01), 51–75.

4. Bjarte, R., Lange, D., Marianthi, T., and Pursiainen, C. (2020). *From risk management to resilience management in critical infrastructure. Journal of Management in Engineering, 36* (4).

5. Alcaraz, C., Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century, International Journal of Critical Infrastructure Protection, 8, 53-66.

6. Pursiainen, C., & Kytömaa, E. (2022). From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure, 8* (1), 85–101.

7. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. *Аналітична доповідь. Національний інститут стратегічних досліджень.* 2012. С. 96.

8. 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.

9. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. *Державне управління: удосконалення та розвиток*. 2022. № 1.

10. Гора І.В., Батюк О.В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії*. 2021. №1 (11). С. 132-139.

11. Братель С. Г. Досвід зарубіжних країн у сфері забезпечення безпеки об'єктів критичної інфраструктури. *Південноукраїнський правничий часопис. Теоретичні та практичні аспекти забезпечення національної безпеки.* 2023. №3. С. 261-265. https://doi.org/10.32850/sulj.2023.3.41.

12. Yefimenko, I., Sakovskyi, A., & Bilozorov, Ye. (2023). Protection of critical infrastructure as a component of Ukraine's national security. *Law Journal of the National Academy of Internal Affairs*. 13(2), 74-85.

13. Герасименко О.М. Загрози об'єктам критичної інфраструктури України в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету*. *Серія Право*. 2024. № 84 (3).

14. Іваницька О., Возненко О. Управління ризиками об'єктів критичної інфраструктури. *Фінанси України*. 2024. № (6), 93-107.

15. Denysov, A. I., Bershov, H. Y., Krykun, V. V., & Zhydovtseva, O. (2021). Protection of Critical Infrastructure Facilities as a Component of the National Security. *Cuestiones Políticas, 39*(71), 789-799.

16. Мельник Д. С. Створення моделі загроз національній критичній інфраструктурі України як основи забезпечення її безпеки та стійкості. *Вісник Харківського національного університету внутрішніх справ*. 2024. № 104 (1(1)), С. 237-250. https://doi:10.32631/v.2024.1.20.

17. Тарасенко Ю. С., Клим В. Ю. Безпека об'єктів критичної інфраструктури з позицій зниження результативності ризиків. *Системні технології.* 2022. № 4 (141).

18. Арсенович Л. А. Деякі питання запровадження системи підготовки фахівців у сфері захисту критичної інфраструктури. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування*. 2023. № 5. С. 3-14. https://doi.org/10.32851/tnv-pub.2022.5.1.

19. 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(15).

20. Скіцько О., Ширшов Р. Система управління інформаційною безпекою як інструмент підвищення захисту та ефективності об'єктів критичної інфраструктури. *Міжнародний науковий журнал інженерії та сільського господарства*. 2023. №*2* (6). С. 12–22.

21. Стародуб, Ю. П., Гаврись, А. П., Ковальчук, В. М., Рогуля, А. О., & Філіппова, В. Досягнення стабільного розвитку територій шляхом реалізації проєкту визначення зон паводкового затоплення в Україні. *Надзвичайні ситуації: попередження та ліквідація*. 2022. №1. С. 103-114

22. Govea, J.; Gaibor-Naranjo, W.; Villegas-Ch, W. (2024). Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience. *Computer, 13,* 122.

23. Lifshitz Sherzer, G.; Urlainis, A.; Moya, S.; Shohet, I. (2024). Seismic Resilience in Critical Infrastructures: A Power Station Preparedness Case Study. *Appl. Sci, 14,* 3835.

24. Мурасов Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. Удосконалення науково-методичного апарату для розрахунку ризиків виникнення та аналізу сценаріїв надзвичайних ситуацій на об'єктах критичної інфраструктури. *Соціальний розвиток і безпека*. 2024. №14 (1). С. 205-217.

25. Гаврись А., Яковчук Р., Стародуб Ю., Тур, Н. Управління ризиками виникнення надзвичайних ситуацій, пов'язаних із затопленням територій на рівні об'єднаних територіальних громад. *Науковий вісник: Цивільний захист та пожежна безпека.* 2023. № (1 (15). С. 101–109.

26. Чумаченко С.М., Кутовий О.П., Попель В.А., Гуйдра О.Г., Заїка Н.В., Мурасов Р.К. Науково-методичний підхід щодо оцінювання безпеки критичної інфраструктури на основі комплексу засобів захисту її об'єктів від БПЛА і крилатих ракет. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки.* 2023. № 1.

27. Азаренко О., Гвоздь В., Гончаренко Ю., Дівізінюк М., Мирошник О., Фаррахов О. Варіант оцінки достовірності та ефективності використання математичної моделі при забезпеченні безпеки об'єкту критичної інфраструктури. *InterConf* 2024. С. 644–655.

28. Мелещенко Р.Г. Інженерно-технічні методи попередження надзвичайних ситуацій техногенного характеру на об'єктах критичної інфраструктури за допомогою оперативного контролю стану повітряного середовища дис. ... д-ра. тех. наук : 21.02.03. Харків, 2020. 378с.

29. Кучма О., Котух Є. Критична інфраструктура та кіберзагрози: досягнення стратегічних цілей державного аудиту щодо кіберзахисту критичної інфраструктури. *Наукові перспективи.* 2023. № 10(40).

30. Тарасенко Ю.С., Савченко І.В. Процеси забезпечення безпеки об'єктів критичної інфраструктури на основі ризику. *Системи та технології.* 2023, № 65(1). С. 67-76.

31. Volkov A., Brechka M., Stadnichenko V., Yaroshchuk V., & Cherkashyn S. (2023). The protection of critical infrastructure facilities from air strikes due to compatible use of various forces and means. *Machinery & Energetics,* 14(4), 23-32.

32. Коцюруба В.І., Білик А. С., Бзот В. Б., Дзеверін І.Г. Захист об'єктів критичної інфраструктури України від прямих влучань ракет за допомогою підземного розташування. *Ядерна та радіаційна безпека*. 2023. № 2(98). С. 69-79.

33. Коцюруба В.І., Білик А.С., Веретнов А.О., Гайдарли Г.С., Борта Р.М., Тертишний Б.І. Методика розрахунків та обґрунтування вимог до інженерного захисту об'єктів критичної інфраструктури від БпЛА типу баражуючий боєприпас. *Опір матеріалів і теорія споруд.* 2022. № 109. С. 164-183.

34. Азаренко О., Гончаренко Ю., Дівізінюк М., Камишенцев Г., Фаррахов О. Деякі аспекти класифікації безпілотних літальних апаратів в інтересах захисту об'єктів критичної інфраструктури. *InterConf*. 2024. 624–637.

35. Азаренко О., Гончаренко Ю., Дівізіньюк М., Мирненко В. Стрілець В. Шляхи підвищення ефективності системи фізичного захисту об'єктів критичної інфраструктури держави, що охороняються. *Журнал наукових праць Соціальний розвиток і безпека*. 2021. №11. С. 200-213.

36. Михайловський Д., Скляров І. Методика розрахунку та інженерного захисту об'єктів критичної інфраструктури та інших стратегічних об'єктів від далекобійних

снарядів. *Міцність матеріалів і теорія конструкцій.* 2023. С. 155–171.

37. Казьмірук С.Д., Леонов Б.Д., Омельян О.С. Забезпечення кібербезпеки об'єктів критичної інфраструктури на основі використання штучного інтелекту в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2024. № 6.

38.Havrys, A., Yakovchuk, R., Pekarska, O., Tur, N. (2024). Use of the computer modelling for the analysis of dangerous areas during flooding of territories. Ecological Engineering & Environmental Technology, 25(4).

References:

1. Statystyka povitrianykh tryvoh. [Statistics of air alarms]. URL: https://air-alarms.in.ua/?from=2022-02-24&to=2024-08-30#statistic [in Ukrainian].

2. Postanova Kabinetu Ministriv Ukrainy Pro zatverdzhennia Poriadku provedennia monitorynhu rivnia bezpeky ob'iektiv krytychnoi infrastruktury pryiniata 22 lyp. 2022 roky № 821 [Resolution of the Cabinet of Ministers of Ukraine on approval of the Procedure for Monitoring the Security Level of Critical Infrastructure Objects adopted on July 22, 2022 No. 821] [in Ukrainian].

3. Shaji George, A., Baskar, T., & Balaji Srikaanth, P. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partners Universal International Innovation Journal*, 02(01), 51–75.

4. Bjarte, R., Lange, D., Marianthi, T., and Pursiainen, C. (2020). From risk management to resilience management in critical infrastructure. *Journal of Management in Engineering*, *36* (4).

5. Alcaraz, C., Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century, *International Journal of Critical Infrastructure Protection*, 8, 53-66.

6. Pursiainen, C., & Kytömaa, E. (2022). From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*, *8* (1), 85–101.

7. Biriukov D. S. (2012). Zakhyst krytychnoi infrastruktury: problemy ta perspektyvy vprovadzhennia v Ukraini. [Protection of critical infrastructure: problems and prospects of implementation in Ukraine]. *Analitychna dopovid. Natsionalnyi instytut stratehichnykh doslidzhen - Analytical report. National Institute of Strategic Studies*, 96.

8. Franchuk V.I., Pryhunov P.Ya., Melnyk S.I. (2021). Bezpeka ob'iektiv krytychnoi infrastruktury v Ukraini: orhanizatsiino-normatyvni problemy ta pidkhody [Security of critical infrastructure facilities in Ukraine: organizational and regulatory problems and approaches]. *Sotsialno-pravovi studii - Social and legal studies*, 3 (13), 142-148 [in Ukrainian].

9. Yaremenko O. I., Strakhnitskyi Ya. O. (2022). Teoretyko-metodychni osnovy zabezpechennia systemy zakhystu krytychnoi infrastruktury derzhavy [Theoretical and methodological foundations of ensuring the system of protection of the state's critical infrastructure]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok - Public administration: improvement and development*, 1 [in Ukrainian].

10. Hora I.V., Batiuk O.V. (2021). Okremi pytannia zakhystu ob'iektiv krytychnoi infrastruktury: zarubizhnyi dosvid [Separate issues of protection of critical infrastructure objects: foreign experience]. *Sotsialno-pravovi studii - Social and legal studies*, 1 (11), 132-139 [in Ukrainian].

11. Bratel S. H. (2023). Dosvid zarubizhnykh krain u sferi zabezpechennia bezpeky ob'iektiv krytychnoi infrastruktury [Experience of foreign countries in the field of ensuring the safety of critical infrastructure facilities]. *Pivdennoukrainskyi pravnychyi chasopys. Teoretychni ta praktychni aspekty zabezpechennia natsionalnoi bezpeky - South Ukrainian legal journal. Theoretical and practical aspects of ensuring national security*, 3, 261-265 https://doi.org/10.32850/sulj.2023.3.41

12. Yefimenko, I., Sakovskyi, A., & Bilozorov, Ye. (2023). Protection of critical infrastructure as a component of Ukraine's national security. *Law Journal of the National Academy of Internal Affairs*, 13(2), 74-85.

13. Herasymenko O.M. (2024). Zahrozy obiektam krytychnoi infrastruktury Ukrainy v umovakh voiennoho stanu [Threats to the objects of critical infrastructure of Ukraine in the conditions of martial law]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia Pravo -Scientific Bulletin of the Uzhhorod National University. Law series*, 84 (3).

14. Ivanytska O., Voznenko O. (2024). Upravlinnia ryzykamy ob'iektiv krytychnoi infrastruktury [Risk management of critical infrastructure facilities]. *Finansy Ukrainy - Finances of Ukraine*, 6, 93-107 [in Ukrainian].

15. Denysov, A. I., Bershov, H. Y., Krykun, V. V., & Zhydovtseva, O. (2021). Protection of Critical Infrastructure Facilities as a Component of the National Security. *Cuestiones Políticas*, *39*(71), 789-799.

16. Melnyk D. S. (2024). Stvorennia modeli zahroz natsionalnii krytychnii infrastrukturi Ukrainy yak osnovy zabezpechennia yii bezpeky ta stiikosti [Creating a model of threats to the national critical infrastructure of Ukraine as a basis for ensuring its security and stability]. *Visnyk Kharkivskoho natsionalnoho universytetu vnutrishnikh sprav -*

Bulletin of Kharkiv National University of Internal Affairs, 104 (1(1)), 237-250. https://doi:10.32631/v.2024.1.20.

17. Tarasenko Yu. S., Klym V. Yu. (2022). Bezpeka ob'iektiv krytychnoi infrastruktury z pozytsii znyzhennia rezultatyvnosti ryzykiv [Safety of critical infrastructure objects from the perspective of risk reduction]. *Systemni tekhnolohii - System technologies*, 4 (141) [in Ukrainian].

18. Arsenovych L. A. (2023). Deiaki pytannia zaprovadzhennia systemy pidhotovky fakhivtsiv u sferi zakhystu krytychnoi infrastruktury [Some issues of introducing a system of training specialists in the field of critical infrastructure protection]. *Tavriiskyi naukovyi visnyk. Seriia: Publichne upravlinnia ta administruvannia - Taurian Scientific Bulletin. Series: Public management and administration*, 5, 3-14. https://doi.org/10.32851/tnv-pub.2022.5.1.

19. Bielai S.V. Yevtushenko I.V. Matsiuk V.V. (2021). Teoretyko-metodolohichni zasady pidhotovky kadriv u sferi zakhystu krytychnoi infrastruktury Ukrainy [Theoretical and methodological principles of personnel training in the field of protection of critical infrastructure of Ukraine]. *Visnyk natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seriia Derzhavne upravlinnia - Bulletin of the National University of Civil Defense of Ukraine. State administration series*, 2(15) [in Ukrainian].

20. Skitsko O., Shyrshov R. (2023). Systema upravlinnia informatsiinoiu bezpekoiu yak instrument pidvyshchennia zakhystu ta efektyvnosti ob'iektiv krytychnoi infrastruktury [Information security management system as a tool for increasing the protection and efficiency of critical infrastructure objects]. *Mizhnarodnyi naukovyi zhurnal inzhenerii ta silskoho hospodarstva - International Scientific Journal of Engineering and Agriculture*, 2 (6), 12–22 [in Ukrainian].

21. Starodub, Y. P., Havrysh, A. P., Kovalchuk, V. M., Rogulia, A. O., & Filipova, V. (2022). Dosiagnennya stabil′noho rozvytku terytoriy shlyakhom realizatsiyi proyektu vyznachennya zon pavodkovoho zatoplennya v Ukrayini. [Achievements of Stable Development of Territories through Implementation of the Project for Determining Flood Zones in Ukraine]. Nadzvychaini sytuatsii: poperedzhennia ta likvidatsiia – Extraordinary situations: prevention and elimination, 1, 103-114 [in Ukrainian].

22. Govea, J.; Gaibor-Naranjo, W.; Villegas-Ch, W. (2024). Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience. *Computer, 13*, 122.

23. Lifshitz Sherzer, G.; Urlainis, A.; Moya, S.; Shohet, I. (2024). Seismic Resilience in Critical Infrastructures: A Power Station Preparedness Case Study. *Appl. Sci, 14*, 3835.

24. Murasov R., Nikitin A., Meshcheriakov I., Pidhorodetskyi M., Poplavets S. (2024). Udoskonalennia naukovo-metodychnoho aparatu dlia rozrakhunku ryzykiv vynyknennia ta analizu stsenariiv nadzvychainykh sytuatsii na ob'iektakh krytychnoi infrastruktury [Improvement of the scientific and methodological apparatus for calculating the risks of occurrence and analyzing scenarios of emergency situations at critical infrastructure facilities]. *Sotsialnyi rozvytok i bezpeka - Social development and security*, 14 (1), 205-217 [in Ukrainian].

25. Havrys A., Yakovchuk R., Starodub Yu., Tur, N. (2023). Upravlinnia ryzykamy vynyknennia nadzvychainykh sytuatsii, pov'iazanykh iz zatoplenniam terytorii na rivni ob'iednanykh terytorialnykh hromad [Management of the risks of emergency situations related to the flooding of territories at the level of united territorial communities]. Naukovyi visnyk: Tsyvilnyi zakhyst ta pozhezhna bezpeka – Scientific bulletin: Civil protection and fire safety, 1 (15), 101–109 [in Ukrainian].

26. Chumachenko S.M., Kutovyi O.P., Popel V.A., Huidra O.H., Zaika N.V., Murasov R.K. (2023). Naukovo-metodychnyi pidkhid shchodo otsiniuvannia bezpeky krytychnoi infrastruktury na osnovi kompleksu zasobiv zakhystu yii ob'iektiv vid BPLA i krylatykh raket [A scientific and methodical approach to assessing the safety of critical infrastructure based on a complex of means of protecting its facilities against UAVs and cruise missiles]. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Tekhnichni nauky - Academic notes of TNU named after V.I. Vernadskyi. Series: Technical sciences*, 1, [in Ukrainian].

27. Azarenko O., Hvozd V., Honcharenko Yu., Diviziniuk M., Myroshnyk O., Farrakhov O. (2024). Variant otsinky dostovirnosti ta efektyvnosti vykorystannia matematychnoi modeli pry zabezpechenni bezpeky ob'iektu krytychnoi infrastruktury [An option for assessing the reliability and effectiveness of using a mathematical model when ensuring the safety of a critical infrastructure object]. *InterConf – InterConf*, 644–655 [in Ukrainian].

28. Meleshchenko R. G. (2020). Engineering and technical methods of prevention of man-made emergencies at critical infrastructure facilities by means of operative control of the air environment. Doctor's thesis. Kharkiv [in Ukrainian].

29. Kuchma O., Kotukh Ye. (2023). Krytychna infrastruktura ta kiberzahrozy: dosiahnennia stratehichnykh tsilei derzhavnoho audytu shchodo kiberzakhystu krytychnoi infrastruktury [Critical infrastructure and cyber threats: achieving the strategic goals of the state audit regarding cyber protection of

critical infrastructure]. *Naukovi perspektyvy - Scientific perspectives*, 10(40) [in Ukrainian].

30. Tarasenko Yu.S., Savchenko I.V. (2023). Protsesy zabezpechennia bezpeky ob'iektiv krytychnoi infrastruktury na osnovi ryzyku [Processes for ensuring the safety of critical infrastructure objects based on risk]. *Systemy ta tekhnolohii - Systems and technologies*, 65(1), 67-76 [in Ukrainian].

31. Volkov A., Brechka M., Stadnichenko V., Yaroshchuk V., & Cherkashyn S. (2023). The protection of critical infrastructure facilities from air strikes due to compatible use of various forces and means. *Machinery & Energetics*, 14(4), 23-32.

32. Kotsiuruba V.I., Bilyk A. S., Bzot V. B., Dzeverin I.H. (2023). Zakhyst ob'iektiv krytychnoi infrastruktury Ukrainy vid priamykh vluchan raket za dopomohoiu pidzemnoho roztashuvannia [Protection of objects of critical infrastructure of Ukraine from direct hits of missiles with the help of underground location]. *Yaderna ta radiatsiina bezpeka - Nuclear and radiation safety*, 2(98), 69-79 [in Ukrainian].

33. Kotsiuruba V.I., Bilyk A.S., Veretnov A.O., Haidarly H.S., Borta R.M., Tertyshnyi B.I. (2022). Metodyka rozrakhunkiv ta obgruntuvannia vymoh do inzhenernoho zakhystu ob'iektiv krytychnoi infrastruktury vid BpLA typu barazhuiuchyi boieprypas [Methodology of calculations and substantiation of requirements for engineering protection of critical infrastructure objects from UAVs of the barrage type]. *Opir materialiv i teoriia sporud - Resistance of materials and theory of structures*, 109, 164-183 [in Ukrainian].

34. Azarenko O., Honcharenko Yu., Diviziniuk M., Kamyshentsev H., Farrakhov O. (2024). Deiaki aspekty klasyfikatsii bezpilotnykh litalnykh aparativ v interesakh zakhystu ob'iektiv krytychnoi infrastruktury [Some aspects of the classification of unmanned aerial vehicles in the interests of protecting critical infrastructure objects]. *InterConf – InterConf*, 624–637 [in Ukrainian].

35. Azarenko O., Honcharenko Yu., Diviziniuk M., Myrnenko V. Strilets V. (2021). Shliakhy pidvyshchennia efektyvnosti systemy fizychnoho zakhystu obiektiv krytychnoi infrastruktury derzhavy, shcho okhoroniaiutsia [Ways to increase the effectiveness of the system of physical protection of protected critical infrastructure objects of the state]. *Zhurnal naukovykh prats Sotsialnyi rozvytok i bezpeka - Journal of scientific works Social development and security*, 11, 200-213 [in Ukrainian].

36. Mykhailovskyi D., Skliarov I. (2023). Metodyka rozrakhunku ta inzhenernoho zakhystu ob'iektiv krytychnoi infrastruktury ta inshykh stratehichnykh ob'iektiv vid dalekobiinykh snariadiv [Methods of calculation and engineering protection of critical infrastructure facilities and other strategic facilities against long-range projectiles]. *Mitsnist materialiv i teoriia konstruktsii - Strength of materials and theory of structures*, 155–171 [in Ukrainian].

37. Kazmiruk S.D., Leonov B.D., Omelian O.S. (2024). Zabezpechennia kiberbezpeky ob'iektiv krytychnoi infrastruktury na osnovi vykorystannia shtuchnoho intelektu v umovakh voiennoho stanu [Ensuring cyber security of critical infrastructure facilities based on the use of artificial intelligence in martial law conditions]. *Yurydychnyi naukovyi elektronnyi zhurnal - Legal scientific electronic journal*, 6 [in Ukrainian].

38. Havrys, A., Yakovchuk, R., Pekarska, O., Tur, N. (2024). Use of the computer modelling for the analysis of dangerous areas during flooding of territories. Ecological Engineering & Environmental Technology, 25(4).

Оглядова стаття.
Надійшла до редакції 17.11.2024.
Прийнято до публікації 18.12.2024.