http://doi.org/10.26565/1727-6667-2024-2-23
УДК 351:355.4:656

Величко Лариса Юріївна,
доктор юридичних наук, професор, завідувач кафедри права,
національної безпеки та європейської інтеграції
Навчально-наукового інституту «Інститут державного управління»
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
ORCID ID: https://orcid.org/0000-0003-3029-4719
e-mail: velychkolara71@gmail.com

Білоконь Михайло Вячеславович,
кандидат наук з державного управління, доцент, доцент закладу вищої освіти кафедри права, національної безпеки та європейської інтеграції
Навчально-наукового інституту «Інститут державного управління»
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
ORCID ID: https://orcid.org/0000-0002-5389-7013
e-mail: m.bilokon@karazin.ua

ГІБРИДНІ ЗАГРОЗИ ТРАНСПОРТНІЙ ІНФРАСТРУКТУРІ: ВИКЛИКИ ДЛЯ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Анотація. В умовах сучасних глобальних викликів транспортна інфраструктура відіграє стратегічну роль у забезпеченні економічної стабільності, мобільності населення, ефективного функціонування ланцюгів постачання та обороноздатності держави. Водночас вона стає мішенню для гібридних загроз, які поєднують кібератаки, фізичні диверсії, інформаційні маніпуляції та економічний тиск. Особливого значення ця проблема набуває для України, яка вже понад десятиліття перебуває в умовах активного гібридного протистояння. Військові дії, спрямовані на руйнування критичної інфраструктури, масовані кібератаки на транспортні мережі, а також зовнішній економічний тиск створюють комплексний виклик для системи державного регулювання та забезпечення національної безпеки.

Актуальність дослідження зумовлена необхідністю розробки ефективних механізмів державної політики, спрямованої на підвищення стійкості транспортної інфраструктури до новітніх загроз. Сьогодні знищення чи виведення з ладу ключових транспортних вузлів здатне не лише завдати значних економічних збитків, а й спричинити соціальну нестабільність, порушити постачання критично важливих ресурсів, ускладнити військову логістику та знизити рівень міжнародної торгівлі. Водночас іноземний досвід свідчить, що інтеграція превентивних заходів, сучасних технологій моніторингу загроз, кіберзахисту та інформаційної безпеки дозволяє мінімізувати вплив гібридних атак на транспортну систему.

У статті здійснено всебічний аналіз основних типів гібридних загроз, які впливають на транспортну інфраструктуру, включаючи: кібератаки на автоматизовані системи управління транспортом, фізичні диверсії проти стратегічних об'єктів (мости, залізничні вузли, аеропорти, морські порти), економічний тиск (санкції, блокування транспортних коридорів) та інформаційно-психологічні операції (дезінформація щодо безпечності транспортних маршрутів, створення паніки, підрив довіри до державних інституцій у сфері транспорту).

Результати дослідження показують, що гібридні загрози мають системний характер і потребують комплексного реагування з боку держави. Проведено оцінку сучасного стану безпеки транспортної інфраструктури України, ідентифіковано її основні вразливості, включаючи недостатню координацію між державними та приватними суб'єктами у сфері транспортної безпеки, застарілість частини нормативно-правової бази, обмежені можливості кризового реагування на масштабні загрози. Запропоновано концептуальну модель стратегії державного регулювання, що охоплює адаптацію українського законодавства до стандартів ЄС та практик НАТО, посилення міжвідомчої координації, розвиток кібербезпеки критичних транспортних об'єктів, інтеграцію сучасних технологій моніторингу загроз та впровадження кризових центрів швидкого реагування.

Окрему увагу приділено аналізу міжнародного досвіду захисту транспортної інфраструктури від гібридних загроз, включаючи стратегії Європейського Союзу, США та країн НАТО щодо забезпечення транспортної безпеки. Обґрунтовано доцільність впровадження в Україні кращих світових практик, зокрема створення державної системи кіберзахисту транспортної галузі, розширення державно-приватного партнерства у сфері безпеки транспортних вузлів та залучення міжнародної технічної допомоги для модернізації критичної інфраструктури.

Запропоновані заходи включають створення загальнонаціональної системи моніторингу транспортної безпеки, імплементацію новітніх стандартів кібербезпеки, інтеграцію технологій штучного інтелекту для виявлення потенційних загроз та розробку механізмів міжнародної співпраці для мінімізації зовнішніх загроз. Окреслено перспективи подальших наукових досліджень у сфері стратегічного управління транспортною безпекою, аналізу ризиків та впровадження нових технологічних рішень для захисту критичної інфраструктури.

Ключові слова: *транспортна інфраструктура; національна безпека; критична інфраструктура; стійкість транспортних систем; безпека логістики; регіональний рівень; національна інфраструктура; залізничний транспорт.*

Як цитувати: Величко Л. Ю., Білоконь М. В. Гібридні загрози транспортній інфраструктурі: виклики для державного регулювання та національної безпеки. *Теорія та практика державного управління*. 2024. Вип. 2 (79). С. 442–464. http://doi.org/10.26565/1727-6667-2024-2-23

Вступ. Транспортна інфраструктура є ключовим елементом економічного та соціального розвитку держави, забезпечуючи мобільність населення, ефективність логістики та функціонування стратегічних секторів економіки. Вона формує основу для регіональної інтеграції, розвитку промисловості, міжнародної торгівлі та національної безпеки. Сучасний рівень глобалізації та взаємо-

залежності економік робить транспортну інфраструктуру критично важливою для стабільності як окремих регіонів, так і держави загалом.

Значення транспортної інфраструктури для регіонального розвитку проявляється у здатності забезпечувати економічне зростання, інвестиційну привабливість та соціальну мобільність населення. Розвинена мережа автомобільного, залізничного, повітряного та водного транспорту сприяє залученню інвестицій, підвищенню конкурентоспроможності регіонів та створенню нових робочих місць. Національний рівень значення транспортної інфраструктури визначається її роллю у забезпеченні економічної безпеки, стратегічного розвитку та обороноздатності країни.

Однак в умовах сучасних геополітичних викликів транспортна інфраструктура стає об'єктом цілеспрямованого впливу гібридних загроз. Гібридні загрози – це комплексні, багатовекторні форми впливу, які поєднують військові, економічні, інформаційні, кібернетичні та соціальні засоби, спрямовані на дестабілізацію держави. Відмінною рисою таких загроз є їхня прихованість, використання методів асиметричного протистояння та націленість на критично важливі сектори економіки та безпеки.

Транспортна інфраструктура є однією з основних цілей гібридних атак, оскільки її виведення з ладу може призвести до значних економічних збитків, соціального хаосу та послаблення обороноздатності держави. Основні форми гібридних загроз у сфері транспорту включають:

– Кібератаки на транспортні системи управління (залізничний транспорт, авіація, морські порти, автомобільні магістралі) з метою порушення їхньої роботи або отримання контролю над ними.

– Фізичні диверсії та саботаж, спрямовані на руйнування стратегічних об'єктів транспортної інфраструктури (мости, тунелі, залізничні вузли, термінали).

– Економічний тиск, що виражається у санкціях, блокаді транспортних коридорів, скуповуванні критичних об'єктів іноземними компаніями, які можуть діяти в інтересах ворожих держав.

– Інформаційні атаки, маніпуляції суспільною думкою та дискредитація транспортних проєктів через дезінформацію та пропаганду.

З огляду на це, питання захисту транспортної інфраструктури від гібридних загроз набуває особливої актуальності для України, яка перебуває в умовах як гібридної війни, так і прямого воєнного вторгнення. Наразі основний виклик полягає у фізичному захисті стратегічних транспортних об'єктів від ракетних ударів, диверсійних операцій та інших засобів збройного впливу. Проте після завершення активної фази бойових дій головну роль знову відіграватимуть саме гібридні методи дестабілізації: кібератаки, економічний тиск, інформаційні операції та приховані диверсії. Повне припинення деструктивних дій проти України у середньостроковій перспективі виглядає малоймовірним, адже гібридний вплив з боку ворога, швидше за все, триватиме принаймні протягом найближчого покоління, що потребує розробки довгострокових механізмів протидії.

Таким чином, дослідження проблематики гібридних загроз для транспортної інфраструктури регіону та аналіз викликів для державного регулювання є

важливим як у науковому, так і у практичному аспекті. Визначення ефективних механізмів протидії таким загрозам сприятиме зміцненню національної безпеки та підвищенню захисту критичної інфраструктури держави.

Огляд літератури. Дослідження гібридних загроз для транспортної інфраструктури активно проводяться як іноземними, так й українськими науковцями. Зокрема, питання кібератак на транспортні системи аналізували Бірман Дж., Берент Д., Фальтер Ц., Бгунія С. [1], Малик З.А., Бутт М.М., Сін Х.М. [2], Шварц М., Маркс М., Федеррат Г. [3], а проблеми розміщення критичної інфраструктури в умовах військових загроз розглядали Боровик К.В., Гапон С.В., Пишнограєв І.О., Хащевацька А.І. [5]. Правові аспекти транспортної інфраструктури висвітлив у свої роботах Гапонов О.О. [7; 8], а гібридним загрозам загалом присвячені роботи авторського колективу у «Глосарії з гібридних загроз» [9] та збірнику «Грані історії» [10]. Взаємозв'язок транспортного сектору з економічним розвитком аналізували Гречан А. [11], Гринь А. [12] та ін., а питання кібербезпеки та її нормативного регулювання досліджували Зубок В.Ю. [13], Кирчата І.М. [14] та ін. Правові механізми протидії гібридним загрозам оцінював Кресін О. [16]. Понятійні аспекти транспортної інфраструктури розглянув Устименко А. [21], а інноваційні підходи до логістики в умовах війни – Целлєр В. та Крамський С. [23]. Рівень безпеки дорожнього руху досліджував Шрамко С.С. [24]. Сукупність цих досліджень формує теоретичну та практичну основу для розробки ефективних механізмів державного регулювання безпеки транспортної інфраструктури в умовах гібридних загроз.

Метою статті є аналіз гібридних загроз транспортній інфраструктурі регіону, визначення їх впливу на національну безпеку та розробка пропозицій щодо удосконалення механізмів державного регулювання для підвищення стійкості критичної інфраструктури.

Методологія дослідження. У ході підготовки наукової статті було використано комплексний підхід, що включає низку взаємодоповнюючих методів дослідження.

По-перше, застосовано системний аналіз, який дозволив всебічно розглянути гібридні загрози транспортній інфраструктурі регіонів у контексті національної безпеки та державного регулювання. Використання цього методу дало змогу оцінити взаємозв'язки між фізичними, інформаційними, кібернетичними та економічними загрозами, а також розглянути їхній вплив на стабільність транспортної системи.

По-друге, використано методи аналізу та синтезу, що дозволили детально опрацювати різні аспекти досліджуваної проблематики, зокрема механізми захисту критичної транспортної інфраструктури, міжнародний досвід у цій сфері та особливості нормативно-правового регулювання. Метод аналізу забезпечив детальне вивчення кожного з елементів системи безпеки, тоді як синтез дозволив інтегрувати отримані дані та сформувати комплексні висновки.

Крім того, застосовано методи узагальнення та деталізації, які сприяли розгляду окремих складових гібридних загроз та інтеграції цих елементів у загальну концепцію транспортної безпеки. Це дозволило виявити основні виклики для державного регулювання, проаналізувати їх у контексті сучасних безпеко-

вих тенденцій та сформулювати рекомендації щодо вдосконалення правового регулювання транспортної інфраструктури.

Також використано метод порівняння, що дозволив проаналізувати приклади гібридних атак на транспортну інфраструктуру України та інших країн, а також оцінити ефективність заходів протидії цим загрозам. Порівняльний аналіз міжнародного досвіду став основою для оцінки можливостей імплементації найкращих практик у сфері транспортної безпеки в українському контексті.

Для вивчення законодавчої бази та регуляторних механізмів було застосовано метод правового аналізу, що дав змогу оцінити відповідність українського законодавства сучасним викликам у сфері транспортної безпеки та визначити напрями його вдосконалення.

Застосування зазначених методів забезпечило комплексний підхід до дослідження проблематики гібридних загроз транспортній інфраструктурі регіонів та дозволило всебічно оцінити виклики для державного регулювання і національної безпеки в цій сфері.

Виклад основного матеріалу. Гібридні загрози є комплексним явищем, що поєднує традиційні та нетрадиційні методи впливу, спрямовані на дестабілізацію держави, підрив її безпеки та ослаблення критично важливих сфер життєдіяльності, зокрема транспортної інфраструктури [9]. Вони виходять за межі класичного розуміння загроз, оскільки не завжди передбачають відкритий збройний конфлікт і часто діють на стику політичних, економічних, інформаційних та військових інструментів впливу.

Головна відмінність між класичними та гібридними загрозами полягає у способах реалізації та ступені прихованості дій.

Класичні загрози – це здебільшого відкриті, прямі дії, такі як військові вторгнення, терористичні атаки або економічні санкції, які мають чітко вираженого суб'єкта та об'єкта протистояння. Вони передбачають формальні оголошення про початок бойових дій, застосування військової сили або введення економічних обмежень із прогнозованими наслідками.

Гібридні загрози – це приховані або комбіновані дії, що використовують взаємопов'язані методи тиску на державу, включаючи кібернапади, інформаційні операції, економічний шантаж, диверсії та підривну діяльність на стратегічних об'єктах. Основна їхня мета – створення нестабільності, підрив довіри до державних інституцій та поступове послаблення країни без відкритого збройного конфлікту або як підготовчий етап до нього.

Особливістю гібридних загроз є їхня комбінована мультидоменна природа [10], яка охоплює як військові, так і невійськові методи впливу. До основних складових гібридних загроз належать:

1. Військовий компонент – може включати застосування нерегулярних військових формувань, диверсійні операції на об'єктах критичної інфраструктури, використання приватних військових компаній або підтримку місцевих антиурядових рухів.

При цьому, військові конфлікти значно впливають на транспортну логістику, руйнуючи критичну інфраструктуру, що ускладнює постачання та збільшує

транспортні витрати. В умовах війни традиційні маршрути стають непридатними для використання, а відновлення інфраструктури є складним завданням через нестачу ресурсів і ризики для ремонтних бригад [23].

2. Кібернетичні атаки – вплив на автоматизовані системи управління транспортом, спроби блокування залізничних мереж, портової інфраструктури або повітряного сполучення через хакерські атаки.

3. Інформаційно-психологічний вплив – поширення дезінформації щодо безпеки транспортних об'єктів, дискредитація державних транспортних проєктів, створення паніки серед населення або маніпуляція суспільною думкою.

4. Економічний шантаж – блокування логістичних ланцюгів, маніпулювання цінами на енергоресурси, санкції або навмисне створення транспортних криз (наприклад, через заборону транзиту товарів).

5. Підривна діяльність та диверсії – атаки на стратегічно важливі мости, тунелі, залізничні вузли, порти та аеропорти, організація аварій або техногенних катастроф із метою паралізувати транспортне сполучення.

Відповідно, гібридні загрози є багаторівневим явищем, що спрямоване на поступове виснаження держави та її критичної інфраструктури. Особливо вразливою до таких атак є транспортна система, оскільки вона відіграє вирішальну роль у функціонуванні економіки, обороноздатності та соціальної стабільності країни. Розуміння особливостей гібридних загроз є ключовим для розробки ефективних механізмів державного регулювання, спрямованих на зміцнення стійкості транспортної інфраструктури.

Гібридні загрози транспортній інфраструктурі є актуальною проблемою для багатьох країн світу. Розглядаючи найбільш характерні приклади таких загроз в різних частинах світу можна виділити їх універсальність для будь-якої країни.

У 2017 році відбулася масштабна кібератака вірусу-здирника NotPetya, яка вразила численні організації в Європі, включаючи транспортні компанії. Зокрема, данська судноплавна компанія Maersk зазнала значних збоїв у роботі своїх інформаційних систем, що призвело до тимчасового припинення операцій у портах по всьому світу. Цей інцидент підкреслив вразливість транспортної інфраструктури до кібератак та необхідність посилення кібербезпеки [3].

У 2021 році Colonial Pipeline, одна з найбільших трубопровідних компаній США, стала жертвою кібератаки із застосуванням програм-вимагачів. Це призвело до тимчасового припинення роботи трубопроводу, який забезпечує близько 45% постачання палива на східному узбережжі США. Інцидент спричинив дефіцит палива та підвищення цін, що підкреслило важливість захисту критичної транспортної інфраструктури від гібридних загроз [1].

У 2019 році в Індії було зафіксовано серію кібератак, які стали частиною гібридної загрози з боку Пакистану. Атаки були спрямовані на енергетичну інфраструктуру та урядові установи Індії, що призвело до тимчасових перебоїв у постачанні електроенергії та порушень у роботі державних служб. Цей випадок підкреслює використання кіберзагроз як частини гібридної війни в Азії [2]. Як Пакистан, так й Індія активно застосовують гібридні методи проти одне одного, у тому числі й щодо транспортної інфраструктури. Відомі випадки спроб кібе-

ратак на залізничні системи та авіаційну інфраструктуру, а також інформаційні кампанії, спрямовані на дискредитацію транспортних ініціатив протилежної сторони. Така ситуація демонструє, що гібридні загрози стають ключовим елементом сучасного міждержавного протистояння, особливо в регіонах із високою геополітичною напруженістю.

Вищенаведені приклади демонструють, що гібридні загрози, зокрема ті що реалізуються через активні кібератаки, становлять серйозну небезпеку для транспортної інфраструктури в різних регіонах світу. Вони підкреслюють необхідність міжнародної співпраці та обміну досвідом у протидії таким загрозам, а також впровадження сучасних технологій та практик для забезпечення стійкості та безпеки транспортних систем.

Очевидно, транспортна інфраструктура є стратегічно важливою складовою економіки та національної безпеки держави. Вона забезпечує мобільність населення, функціонування ланцюгів постачання, розвиток міжнародної торгівлі та стабільність критичних секторів, зокрема оборонної сфери. Водночас така інфраструктура є вразливою до гібридних загроз, які можуть дестабілізувати країну та поставити під загрозу її економічну і політичну стійкість – як це було згадано вище. У цьому контексті роль держави у забезпеченні безпеки транспортної інфраструктури є ключовою.

Державне регулювання безпеки транспортної інфраструктури може реалізовуватись через нормативно-правове регулювання та інституційні механізми забезпечення безпеки.

Нормативно-правова база є основою для створення ефективної системи безпеки транспортної інфраструктури. Держава через законодавчі акти визначає вимоги до стійкості транспортних об'єктів, заходи захисту від загроз, процедури реагування на кризові ситуації та механізми міжнародної співпраці у сфері безпеки.

Основні аспекти законодавчого регулювання включають: закони та нормативно-правові акти які регламентують вимоги до фізичного та кібернетичного захисту транспортних об'єктів; впровадження норм і стандартів захисту інформаційних систем які керують транспортними мережами; законодавче закріплення процедур управління кризами, включаючи координацію між правоохоронними органами, військовими структурами та приватним сектором; участь у міжнародних угодах та програмах співпраці у сфері безпеки транспорту, зокрема в межах ООН, НАТО, ЄС тощо.

Для реалізації державної політики у сфері безпеки транспортної інфраструктури має діяти розгалужена система інституційних механізмів яка включає державні органи, правоохоронні структури, спеціалізовані агентства та приватний сектор.

Ключовими елементами такої системи є:

– Національні агентства з транспортної безпеки – спеціалізовані державні органи, що здійснюють контроль за безпекою транспортних мереж, розробляють стандарти безпеки та координують заходи щодо протидії загрозам.

– Служби розвідки та контррозвідки – виявлення та попередження потенційних загроз, зокрема диверсій, кібернападів та терористичних актів.

– Правоохоронні органи – реалізація оперативних заходів щодо забезпечення фізичної безпеки транспортних вузлів, аеропортів, морських портів та залізничних об'єктів.

– Збройні сили та сили територіальної оборони – залучення військових структур до захисту стратегічно важливих транспортних об'єктів у періоди криз та збройних конфліктів.

– Приватний сектор – співпраця держави з приватними транспортними компаніями та операторами інфраструктури щодо кібербезпеки, фізичного захисту об'єктів та кризового реагування.

Ефективна взаємодія між цими структурами дозволяє державі швидко реагувати на гібридні загрози, запобігати їхньому розвитку та мінімізувати можливі наслідки для транспортної інфраструктури та національної безпеки. Відповідно, державна політика у сфері безпеки транспортної інфраструктури повинна базуватися на чітко визначених законодавчих нормах та ефективній інституційній взаємодії, що забезпечуватиме стійкість транспортної системи до сучасних гібридних загроз.

Україна приділяє значну увагу забезпеченню безпеки транспортної інфраструктури та протидії гібридним загрозам, розробляючи відповідну нормативно-правову базу та впроваджуючи державні стратегії.

Міністерство інфраструктури України було головним органом у системі центральних органів виконавчої влади, який забезпечував формування та реалізацію державної політики з питань безпеки на автомобільному, міському електричному, залізничному, морському та річковому транспорті [17]. Міністерство інфраструктури України зазнало кількох реорганізацій та перейменувань. У грудні 2022 року Кабінет Міністрів об'єднав Міністерство інфраструктури з Міністерством розвитку громад та територій, утворивши Міністерство розвитку громад, територій та інфраструктури України. У вересні 2024 року відбулася чергова зміна: Міністерство розвитку громад, територій та інфраструктури України було перейменовано на Міністерство розвитку громад та територій України. Таким чином, на сьогодні Міністерство розвитку громад та територій України відповідає за питання, пов'язані з розвитком громад та територій, тоді як функції, пов'язані з інфраструктурою, можуть бути перерозподілені або перебувати в процесі реорганізації.

Кабінет Міністрів України схвалив низку стратегічних документів, спрямованих на підвищення безпеки на транспорті. Ці документи визначають основні напрями державної політики у сфері транспортної безпеки та встановлюють заходи для досягнення поставлених цілей, зокрема:

1. Національна транспортна стратегія України на період до 2030 року та операційний план заходів з її реалізації у 2025-2027 роках [19]. Оновлена Стратегія спрямована на підвищення інституційної спроможності органів управління транспортним сектором, розвиток людського капіталу та цифровізацію галузі. Ці заходи сприятимуть реалізації галузевих реформ та підтримці євроінтеграційного курсу України. Серед ключових завдань Стратегії у сфері безпеки виділяються: приведення національного законодавства у відповідність до

актів права ЄС; впровадження міжнародних стандартів безпеки на транспорті; інтеграція національної транспортної мережі до Транс'європейської транспортної мережі (TEN-T); гармонізація з пріоритетами Європейського зеленого курсу в секторі транспорту і мобільності. Ці заходи спрямовані на підвищення безпеки транспортної інфраструктури, зменшення аварійності та забезпечення стійкості транспортної системи України перед сучасними викликами.

2. Стратегія підвищення рівня безпеки дорожнього руху на період до 2024 року [20]. Ключовою метою цієї Стратегії є зниження рівня смертності внаслідок дорожньо-транспортних пригод (ДТП) щонайменше на 30% до 2024 року та на 50% до 2030 року порівняно з показниками 2019 року. Для досягнення поставлених цілей Стратегія передбачає комплекс заходів, зокрема: розвиток інфраструктури безпеки, підвищення ефективності контролю за дотриманням правил дорожнього руху (впровадження сучасних систем автоматичного контролю та посилення відповідальності за порушення), покращення якості дорожньої інфраструктури (ремонт та модернізація доріг з урахуванням безпекових стандартів, встановлення сучасних засобів організації дорожнього руху), підвищення обізнаності учасників дорожнього руху (проведення інформаційно-просвітницьких кампаній щодо безпеки на дорогах). Реалізація цих заходів спрямована на зменшення кількості ДТП, зниження травматизму та смертності на дорогах України, а також на підвищення загального рівня безпеки дорожнього руху.

Реалізація Стратегії підвищення рівня безпеки дорожнього руху в Україні на період до 2024 року зазнала значних викликів у зв'язку з повномасштабним вторгненням. Військові дії призвели до руйнування транспортної інфраструктури, зміни маршрутів руху та появи нових небезпек на дорогах.

За даними дослідження, опублікованого у 2024 році, у перший рік повномасштабного вторгнення додалися нові чинники небезпеки на дорогах. Зокрема, у 2023 році в Україні сталося 23 642 ДТП із загиблими та/або травмованими, що на 26,9% більше, ніж у 2022 році. Кількість загиблих зросла на 9,4%, а травмованих – на 27,5% [24].

Ці показники свідчать про те, що досягнення цілей Стратегії стало вкрай складним завданням в умовах війни. Військові дії внесли корективи у пріоритети державної політики, спричинивши перенаправлення ресурсів на оборону та відновлення критичної інфраструктури.

В цілому, українське законодавство у сфері національної безпеки, включаючи протидію гібридним загрозам, відзначається концептуальною комплексністю. Воно регулює основні сфери реальних і потенційних загроз, розглядаючи їх у нерозривному зв'язку зовнішніх і внутрішніх чинників, суб'єктності держави, суспільства та громадянина. Законодавство спрямоване не лише на збереження функціонування держави й життєдіяльності суспільства, а й на захист демократичного розвитку, прав і свобод людини, притаманних українському суспільству цінностей [16]. Тож, й сучасне правове регулювання транспортної безпеки в Україні має певні досягнення, проте в умовах гібридних загроз воно потребує подальшого вдосконалення. Специфіка гібридних загроз, які поєднують військові та невійськові методи впливу, створює нові виклики для транспортної

інфраструктури. Існуючі нормативно-правові акти не завжди враховують ці сучасні виклики та потребують оновлення з урахуванням новітніх загроз.

Здатність держави ефективно реагувати на гібридні загрози у сфері транспортної інфраструктури визначається рівнем розвитку її інституційної спроможності. До ключових суб'єктів забезпечення транспортної безпеки належать силові структури, розвідувальні органи, кіберзахистові підрозділи, а також державні та приватні оператори транспортної галузі.

Силові структури (Збройні Сили України, Національна гвардія, Національна поліція, Державна прикордонна служба) відіграють критично важливу роль у забезпеченні фізичної безпеки транспортної інфраструктури, особливо в умовах війни та гібридних атак. Зокрема: ЗСУ та НГУ здійснюють захист критичної транспортної інфраструктури (мостів, залізничних вузлів, аеропортів) від можливих диверсій та прямих військових ударів. Національна поліція та Держспецзв'язку забезпечують оперативне реагування на кібератаки та фізичні загрози. Державна прикордонна служба контролює перетин кордону, запобігаючи незаконному переміщенню осіб та вантажів, що можуть бути задіяні у гібридних атаках.

Головне управління розвідки МО України (ГУР МОУ) та Служба безпеки України (СБУ) відіграють ключову роль у виявленні загроз та запобіганні гібридним атакам, зокрема:

– Моніторинг активності ворожих спецслужб та терористичних груп у сфері транспорту.

– Протидія інформаційним і дезінформаційним кампаніям, що спрямовані на дестабілізацію транспортної системи.

– Виявлення та нейтралізація фінансових і логістичних каналів, які можуть використовуватися для гібридних операцій.

Останнім часом спостерігається зростання кількості кібератак на транспортні системи, включаючи. Атаки на залізничну систему, що можуть спричинити збої в перевезеннях. Злам систем керування рухом аеропортів та портів. Використання шкідливого програмного забезпечення для дестабілізації міського транспорту. Тож, захист транспортної кіберінфраструктури здійснюють:

– Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) – відповідальна за розробку та реалізацію заходів кіберзахисту.

– Національний координаційний центр кібербезпеки (НКЦК) при РНБО, що координує зусилля у сфері кібербезпеки.

– Кіберпідрозділи СБУ та МВС, які займаються реагуванням на кіберзагрози.

Ефективний захист транспортної інфраструктури неможливий без співпраці між державними установами та приватним сектором. «Укрзалізниця», морські порти, авіакомпанії та міські транспортні системи мають бути інтегрованими у загальнодержавну систему реагування на гібридні загрози. Спільні навчання між силовими структурами та операторами транспорту допомагають відпрацьовувати алгоритми дій у разі надзвичайних ситуацій. Приватні перевізники та логістичні компанії повинні мати доступ до оперативної інформації про можливі загрози та діяти відповідно до національних протоколів безпеки.

Хоча Україна має розгалужену систему забезпечення транспортної безпеки, інституційна спроможність держави потребує подальшого зміцнення. Необхідне вдосконалення координації між державними структурами, розвиток кібербезпеки та посилення міжнародної співпраці для ефективної протидії гібридним загрозам у транспортній сфері.

Захист критичної транспортної інфраструктури в умовах гібридних загроз вимагає комплексного, багаторівневого підходу, який інтегрує фізичні заходи, кіберзахист, правові інструменти, організаційні структури та інформаційну протидію. Сучасні заходи з безпеки орієнтовані на те, щоб унеможливити як прямі, так і приховані дії ворога, здатні порушити нормальне функціонування транспортних систем. Фізичний захист забезпечується впровадженням систем відеоспостереження, сигналізації, контролю доступу та інших інженерних рішень, які дозволяють захистити стратегічні об'єкти, такі як мости, залізничні вузли, аеропорти та порти, від можливих диверсій та атак. Одночасно проводиться регулярне технічне обслуговування та модернізація об'єктів інфраструктури, що сприяє підвищенню їхньої стійкості до руйнувальних дій.

Оптимальне розташування критичної інфраструктури, зокрема транспортних об'єктів, відіграє ключову роль у забезпеченні національної безпеки в умовах військових загроз. Використання ГІС-моделювання дозволяє оцінити придатність територій для розміщення критично важливих об'єктів, враховуючи доступність транспортних шляхів, близькість до стратегічних ресурсів і віддаленість від зон активних бойових дій [5].

У сфері кібербезпеки створюються системи постійного моніторингу інформаційних мереж, які управляють транспортними процесами. Це дозволяє оперативно виявляти кібератаки, зокрема спроби зламу систем керування рухом або саботажу, а також вчасно впроваджувати заходи для нейтралізації загроз. Сучасні протоколи безпеки постійно вдосконалюються шляхом оновлення програмного забезпечення, застосування шифрування і багатофакторної аутентифікації, а також через регулярні тренінги та симуляції кіберінцидентів для підвищення кваліфікації спеціалістів.

Правовий аспект захисту транспортної інфраструктури теж не залишається осторонь. Як було вказано раніше, існуюча нормативно-правова база в Україні охоплює основні сфери безпеки, проте вона потребує подальшої адаптації до сучасних викликів, які виникають у зв'язку з гібридними загрозами. Модернізація законодавства та розробка спеціалізованих стандартів є необхідними кроками для того, щоб встановити чіткі обов'язки всіх суб'єктів, які беруть участь у захисті критичних об'єктів, і забезпечити ефективну правову підтримку оперативного реагування.

Організаційний рівень захисту базується на створенні кризових центрів і оперативних груп, що об'єднують зусилля силових структур, розвідувальних органів, кіберпідрозділів і представників приватного сектору. Така інтеграція дозволяє забезпечити міжвідомчу координацію дій під час кризових ситуацій, спричинених як прямими, так і гібридними загрозами. Співпраця державних і приватних операторів транспорту, спільні навчання та обмін інформацією значно підвищують рівень готовності до реагування на будь-які інциденти.

Водночас, інформаційна протидія є невід'ємною складовою захисної системи, оскільки сучасні гібридні загрози часто включають елементи дезінформації та психологічного впливу. Контроль за інформаційним простором і проведення цілеспрямованих комунікаційних кампаній допомагають запобігати паніці та сприяють підвищенню обізнаності громадськості щодо заходів безпеки.

Оскільки гібридні загрози поєднують традиційні військові методи з сучасними кібернетичними та інформаційними атаками, захисні механізми мають бути надзвичайно гнучкими та адаптивними. Використання інноваційних технологій, таких як штучний інтелект і машинне навчання, дозволяє автоматизувати процеси виявлення аномалій і оперативного реагування на загрози, що є критично важливим для своєчасного коригування заходів безпеки.

У період з 2014 по 2024 роки Україна зазнала низки гібридних атак, спрямованих на її транспортну інфраструктуру. Ці атаки включали як фізичні диверсії, так і кібератаки, що мали на меті дестабілізувати логістичні та транспортні системи країни [22].

У грудні 2016 року відбулася кібератака на енергетичну інфраструктуру Києва, яка призвела до тимчасового відключення електропостачання в частині столиці. Ця атака вплинула на роботу транспортних систем, зокрема світлофорів та електротранспорту, створюючи додаткові ризики для безпеки руху [4].

У 2022 році, після початку повномасштабного вторгнення, російські хакери здійснили серію кібератак на українські логістичні компанії та державні установи, відповідальні за транспорт. Ці атаки були спрямовані на порушення ланцюгів постачання, дезорганізацію перевезень та створення хаосу в управлінні транспортними потоками.

У період з 22 березня до 31 серпня 2024 року збройні сили російської федерації здійснили дев'ять хвиль добре скоординованих комбінованих ракетних атак на енергетичну інфраструктуру України, пошкодивши або зруйнувавши численні об'єкти генерації, передачі та розподілу електроенергії. Ці удари спричинили серйозні довготривалі наслідки, завдавши шкоди цивільному населенню та ключовим системам, включаючи транспортну інфраструктуру [6].

Варто підкреслити, що через воєнні дії на території України транспортна система та інфраструктура зазнають значних руйнувань і пошкоджень. Удари по дорогах, залізничних магістралях, мостах, аеропортах та інших стратегічних об'єктах спричиняють суттєві труднощі в переміщенні людей і транспортуванні вантажів [8].

Гібридні атаки на транспортну інфраструктуру України мали комплексний характер, поєднуючи фізичні диверсії та кібератаки, що вимагало від держави впровадження багаторівневих механізмів захисту та швидкого реагування на нові виклики.

Інформаційні атаки в межах гібридної війни можуть бути не менш руйнівними, ніж кібернетичні чи фізичні напади на транспортну інфраструктуру. Дезінформаційні кампанії здатні підірвати довіру суспільства до державних інституцій, спровокувати паніку та дестабілізувати ситуацію в країні.

Під час активних бойових дій російські пропагандисти поширювали неправдиву інформацію про нібито обстріли українськими військовими евакуаційних коридорів або блокування шляхів евакуації. Це створювало недовіру до офіційних повідомлень та ускладнювало процес евакуації цивільного населення [15].

У деяких випадках поширювалися неправдиві повідомлення про нібито зруйновані мости, дороги чи залізничні колії, що насправді були в робочому стані. Це могло призводити до хаосу в логістиці та паніки серед населення. Російські дезінформаційні кампанії часто спрямовані на підрив довіри до інфраструктурних ініціатив в Україні. Наприклад, поширювалися фейкові новини про корупцію або неякісне виконання робіт у рамках великих транспортних проєктів, що мало на меті знизити підтримку громадськості та міжнародних партнерів.

Транспортна інфраструктура, зокрема морські порти та авіаційні перевезення, є критично важливими для економічної стійкості держави. В умовах гібридної війни ці сектори стають об'єктами цілеспрямованого тиску через економічні санкції, блокування торговельних маршрутів, інформаційні атаки та прямі диверсійні дії. Еволюція загроз для морського та авіаційного транспорту можна розглядати у трьох фазах: період гібридної війни до 2022 року, період повномасштабного вторгнення та майбутні виклики у фазі нової «холодної війни».

1. Після анексії Криму у 2014 році Росія розпочала систематичний гібридний тиск на морське судноплавство в Чорному та Азовському морях. Це включало: блокування Керченської протоки та навмисне створення затримок для українських суден, що заходили у порти Бердянська та Маріуполя; формальні перевірки та зупинки суден під приводом «безпекових заходів», що спричиняло фінансові втрати для судноплавних компаній; дезінформаційні кампанії про «небезпечність» українських портів для міжнародних перевізників, що підривало їхню конкурентоспроможність.

У цей же період гібридний тиск на авіацію України здійснювався через: обмеження повітряного простору над окупованими територіями та Кримом, що змушувало авіакомпанії змінювати маршрути; дипломатичний та економічний тиск на міжнародних перевізників, спрямований на те, щоб вони уникали польотів до українських аеропортів; дезінформаційні кампанії про нібито небезпечний стан аеропортів та ненадійність українського авіапростору.

2. Після лютого 2022 року Росія перейшла до відкритої блокади українських портів, оголосивши північно-західну частину Чорного моря «зоною воєнних дій». Основні наслідки включають: мінування акваторій, що унеможливило нормальну роботу цивільного судноплавства; фізичні атаки на порти, зокрема обстріли Одеси, Чорноморська, Миколаєва та інших припортових міст; зрив зернової угоди у 2023 році, що вплинуло на глобальний ринок продовольства та економічну ситуацію в Україні.

В той же час, після початку вторгнення Україна була змушена закрити свій авіапростір для цивільної авіації. Основні ризики включають: знищення аеро-

портів, що відбулося в перші місяці війни (Гостомель, Харків, Вінниця, Чернігів, Миколаїв); загроза ракетних ударів, що унеможливлює відновлення повноцінних комерційних авіаперевезень у найближчій перспективі; відмова страхових компаній страхувати польоти над Україною, що означає економічні труднощі для авіаперевізників навіть після закінчення війни.

3. Навіть після завершення активних бойових дій морське судноплавство України залишатиметься під тиском Росії через: гібридні загрози мінування акваторій та навмисне поширення фейкових повідомлень про «небезпечність» чорноморських маршрутів; вплив на міжнародних страхувальників з метою завищення страхових ставок для українських суден, що ускладнить торговельні операції; дипломатичний тиск через лояльні до Росії країни, які можуть просувати обмеження щодо морських перевезень з України.

Після деескалації бойових дій Україна зіткнеться й з низкою гібридних загроз у сфері авіаперевезень: спроби Росії через міжнародні структури блокувати відновлення авіасполучення України, поширюючи інформацію про «небезпечний повітряний простір»; вплив на міжнародні страхові компанії, що можуть встановити завищені тарифи на страхування польотів над Україною; фальшиві інформаційні кампанії про нібито теракти чи загрози на авіаційних маршрутах, які можуть підірвати довіру до українських аеропортів.

Ефективною відповіддю на ці загрози стане подальша інтеграція України в міжнародні транспортні ініціативи, посилення присутності військово-морських сил партнерів у Чорному морі та міжнародні юридичні кроки для відновлення судноплавства. Україна повинна активно працювати з міжнародними авіаційними організаціями, запроваджувати жорсткі стандарти безпеки та інвестувати у відновлення аеропортів і технологічну модернізацію галузі.

Крім того, транспортна інфраструктура є ключовим фактором економічного розвитку регіонів, впливаючи на їхню інтеграцію у глобальний ринок, підвищення конкурентоспроможності та мобільності населення. Водночас управління дорожнім господарством стикається з проблемами недостатнього фінансування, зношеності інфраструктури та неефективності управлінських процесів, що вимагає впровадження інноваційних технологій та стратегічного планування [12] – враховуючи те що транспортна інфраструктура відіграє ключову роль у забезпеченні сталого розвитку економіки, сприяючи її конкурентоспроможності, соціальній стабільності та інтеграції у глобальний ринок. В умовах гібридних загроз та економічної турбулентності модернізація транспортного сектору має базуватися на принципах енергоефективності, цифровізації та впровадження екологічних технологій [11].

По мірі того, як активні бойові дії поступово перейдуть у фазу гібридної війни, Україна зіткнеться із новими викликами, схожими на ті, що мали місце у період «холодної війни» XX століття. Основні механізми тиску на транспортну інфраструктуру включатимуть міжнародні торговельні та страхові обмеження, що можуть використовуватись як економічна зброя; підрив довіри до українських перевізників через інформаційні кампанії та асиметричні кібератаки на логістичні та управлінські системи транспортної галузі.

Завданням України буде розбудова стійких транспортних коридорів, адаптованих до нових реалій, а також активна робота із західними партнерами щодо гарантій безпеки для перевізників та інвесторів у транспортну сферу.

В умовах сучасних викликів, коли гібридні загрози становлять комплексну небезпеку для транспортної інфраструктури, Україна потребує суттєвого вдосконалення законодавчої бази. Поточні нормативно-правові акти, що регулюють питання безпеки критичної інфраструктури, були розроблені здебільшого у довоєнний період і не повною мірою враховують специфіку новітніх загроз. Враховуючи це, вдосконалення законодавства має відбуватися комплексно – у кількох основних напрямах.

1. Одним із ключових пріоритетів може стати внесення змін у законодавство, яке чітко визначатиме статус транспортної інфраструктури як критичної складової національної безпеки. Хоча в Україні вже існують певні правові акти, що стосуються загальної критичної інфраструктури, вони не деталізують специфіку загроз саме для транспортної сфери та механізми її захисту.

На сьогодні в Україні вже створено правову основу для регулювання різних видів транспорту завдяки ухваленню базового Закону України «Про транспорт» та низки інших нормативно-правових актів, що визначають порядок функціонування окремих транспортних секторів. Це суттєвий крок у забезпеченні стабільності та ефективності транспортної системи. Водночас, з огляду на динамічний розвиток галузі, правові механізми потребують постійного оновлення та вдосконалення. Технологічний прогрес, зміни в економічному середовищі та суспільні запити вимагають адаптації законодавства до сучасних реалій [7].

Більше того, різноманітність підходів навіть до визначення терміна «транспортна інфраструктура» свідчить про необхідність його уніфікації для формування єдиного розуміння, що є особливо актуальним у процесі відновлення України. Зміни у світових економічних зв'язках уже спричинили трансформацію функцій і складу транспортної інфраструктури, що потребує чіткої термінологічної визначеності [21].

2. Ще одним важливим напрямом реформування законодавчої бази має стати адаптація українських нормативних актів до стандартів НАТО та ЄС. Це дозволить не лише підвищити рівень безпеки транспортної інфраструктури, а й забезпечить її інтеграцію у європейську транспортну мережу, що є стратегічно важливим для економічного розвитку країни.

Зокрема, 14 листопада 2024 року до Верховної Ради України було подано проєкт Закону №12208 «Про внесення змін до Закону України «Про критичну інфраструктуру» щодо імплементації положень Директиви (ЄС) 2022/2557 Європейського парламенту та Ради від 14 грудня 2022 року про стійкість критично важливих об'єктів і скасування Директиви Ради 2008/114/ЕС» [18]. Цей законопроєкт спрямований на адаптацію українського законодавства до новітніх стандартів ЄС у сфері захисту критичної інфраструктури.

Запровадження стандартів НАТО щодо захисту транспортних коридорів: у межах програм НАТО передбачено чіткі протоколи безпеки для залізничних перевезень, морських портів та авіаційної інфраструктури в умовах військо-

вих і гібридних загроз. Їхнє впровадження дозволить підвищити рівень захисту транспортних шляхів.

Застосування спільних кібербезпекових норм ЄС: у Європі діє жорстке законодавство щодо кібербезпеки критичних об'єктів (Директива NIS2). Україна має гармонізувати своє законодавство із цими нормами, посилюючи контроль над цифровими системами управління транспортом.

Директива ЄС 2022/2555, відома як NIS2, набула чинності 16 січня 2023 року, замінивши попередню Директиву 2016/1148 (NIS). Вона спрямована на підвищення рівня кібербезпеки в Європейському Союзі, розширюючи сферу дії та встановлюючи більш суворі вимоги до безпеки та звітності про інциденти. Станом на сьогодні, Директива NIS2 не була безпосередньо імплементована в українське законодавство. Однак, Україна активно працює над гармонізацією свого законодавства у сфері кібербезпеки з європейськими стандартами. Зокрема, у травні 2023 року було укладено науково-технічну роботу з Міністерством освіти і науки України, яка передбачає аналіз та адаптацію положень NIS2 до національних реалій [13].

Розширення міжнародної координації у сфері транспортної безпеки: Україна має брати активну участь у механізмах ЄС щодо обміну інформацією про потенційні загрози (таких як EU Intelligence and Situation Centre) та запроваджувати європейські механізми попередження гібридних загроз.

3. Окремим критично важливим напрямом вдосконалення законодавства має стати прийняття стандартів кібербезпеки для всіх об'єктів транспортної інфраструктури. На сьогодні Україна вже має законодавчі ініціативи у сфері кібербезпеки, проте вони не враховують специфіку загроз для транспортного сектору. Мова має йти про впровадження обов'язкового аудиту кібербезпеки для операторів транспортної інфраструктури – кожна компанія, яка управляє стратегічними транспортними об'єктами, має проходити регулярний контроль відповідності сучасним стандартам кіберзахисту.

Критичною є розробка єдиних стандартів шифрування та протоколів доступу – управління цифровими системами транспортної інфраструктури має здійснюватися за допомогою захищених каналів комунікації, що унеможливить несанкціоноване втручання у транспортні процеси. Крім того, актуальним є створення загальнонаціональної платформи обміну інформацією про кіберзагрози – необхідно забезпечити ефективну комунікацію між державними органами, приватним сектором та міжнародними партнерами для швидкого виявлення атак та їхньої нейтралізації.

4. Захист транспортної інфраструктури неможливий без активної участі приватного сектору, адже значна частина стратегічних об'єктів перебуває у приватному володінні або управлінні. Тому необхідно законодавчо закріпити механізми співпраці між державою та приватним бізнесом у питаннях забезпечення безпеки. Регулярне проведення навчань між представниками держави та приватного сектору підвищить ефективність реагування у разі надзвичайних ситуацій.

Важливим є використання державно-приватного партнерства як інструменту реалізації ефективних проєктних рішень у процесі відновлення транспортної інфраструктури України. Впровадження проєктного підходу сприятиме за-

лученню інвестицій та підвищенню ефективності управління інфраструктурними проєктами [14].

Необхідною є розробка системи страхування на випадок атак або саботажу, яка зменшить фінансові втрати для перевізників та інвесторів. В той же час, держава може запровадити податкові пільги для компаній, які впроваджують високі стандарти кібер- та фізичної безпеки.

Висновки з даного дослідження і перспективи подальших досліджень. Транспортна інфраструктура є ключовим елементом національної безпеки та економічної стабільності країни. Вона забезпечує безперебійне функціонування логістичних ланцюгів, мобільність населення та підтримку обороноздатності держави. В умовах гібридних загроз транспортна система стає мішенню для комплексного впливу, який включає фізичні руйнування, кібератаки на логістичні центри, інформаційні маніпуляції та економічний тиск через блокування транспортних маршрутів. Ці загрози є багатовимірними, що підтверджується світовим досвідом атак на транспортні системи в ЄС, США, Азії. Аналіз доводить, що стратегічне державне регулювання є одним із головних інструментів протидії таким викликам, а законодавче забезпечення безпеки транспорту має бути постійно оновлюваним та адаптованим до нових реалій.

Сучасне українське законодавство у сфері транспортної безпеки створює правову основу для регулювання галузі, проте потребує значного вдосконалення. Попри наявність базового Закону України «Про транспорт» та інших нормативних актів, досі не ухвалено спеціального закону про захист критичної транспортної інфраструктури, що чітко визначав би механізми захисту, координації та відповідальності між державними органами, операторами транспорту та міжнародними партнерами. Крім того, наявна інституційна структура управління безпекою транспорту є недостатньо скоординованою, що ускладнює ефективне реагування на гібридні загрози. Водночас адаптація українського законодавства до стандартів ЄС та НАТО у сфері транспортної безпеки та кіберзахисту стала нагальною потребою.

До основних викликів для державного регулювання та національної безпеки в умовах гібридних загроз належать фізичне руйнування транспортної інфраструктури, зростаючий рівень кібератак на логістичні системи, інформаційні кампанії, спрямовані на дискредитацію транспортних проєктів, а також економічний тиск через блокування портів і транспортних коридорів. Сучасні воєнні дії в Україні спричинили масштабне знищення стратегічно важливих об'єктів, включаючи мости, дороги, аеропорти та залізничні вузли, що ускладнило переміщення людей і товарів та призвело до значних економічних втрат. Крім того, інформаційна війна, що супроводжується поширенням фейкових новин про нібито повну непридатність української транспортної мережі або корупційні схеми в її відновленні, спричиняє зниження довіри до державних інститутів та міжнародних інвесторів.

Повернення активної фази війни у формат гібридного протистояння загрожує довготривалим тиском на транспортний сектор через дипломатичні, економічні та інформаційні інструменти. Росія може продовжувати перешкоджати

страхуванню українських суден, поширювати дезінформацію про небезпеку повітряного простору України для міжнародних авіаперевізників та блокувати логістичні маршрути. У цих умовах необхідним є впровадження комплексних заходів захисту транспортної інфраструктури, що включають удосконалення кіберзахисту, покращення міжвідомчої координації, створення кризових центрів оперативного реагування, імплементацію міжнародних стандартів захисту та розширення співпраці з партнерами НАТО та ЄС.

Сучасні виклики вимагають не лише фізичного відновлення інфраструктури, а й посилення її захисту від новітніх загроз. Це означає необхідність ухвалення стратегічних документів, що закріплять довгострокові механізми безпеки, зокрема створення загальнонаціональної системи моніторингу та аналізу загроз для транспортної інфраструктури. Інвестиції у модернізацію транспортних об'єктів, цифровізацію управління та впровадження міжнародних стандартів безпеки є ключовими елементами, що сприятимуть підвищенню стійкості транспортної системи та її інтеграції у глобальні транспортні мережі. Ефективна державна політика, комплексне оновлення законодавства та залучення міжнародних ресурсів можуть створити надійний фундамент для захисту української транспортної інфраструктури від гібридних загроз у майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.

1. Beerman J., Berent D., Falter Z., Bhunia S. A Review of Colonial Pipeline Ransomware Attack. 2021. URL: https://ieeexplore.ieee.org/abstract/document/10181159/authors#authors
2. Malik Z.A., Butt M.M., Xing H.M., Nazir B., Shabbir S., Fatima H., Khan A.U., Zheng M. Cyber Warfare from Pakistan-India: A Critical Analysis. *International Journal of Special Education*. Vol.37, No.3, 2022. URL: https://www.researchgate.net/profile/Sundas-Malik/publication/373737800_Cyber_Warfare_from_Pakistan-India_A_Critical_Analysis/links/64fa10dfe098013a83decaa6/Cyber-Warfare-from-Pakistan-India-A-Critical-Analysis.pdf
3. Schwarz M., Marx M., Federrath H. A Structured Analysis of Information Security Incidents in the Maritime Sector. 2021. DOI: https://doi.org/10.48550/arXiv.2112.06545
4. The Ukrainian Power Grid Was Hacked Again. URL: https://web.archive.org/web/20170118201525/http://motherboard.vice.com/read/ukrainian-power-station-hacking-december-2016-report
5. Боровик К.В., Гапон С.В., Пишнограєв І.О., Хащевацька А.І. Моделювання придатності територій для розміщення критичної інфраструктури України в умовах військових загроз. *Український журнал дистанційного зондування Землі*, 2024, 11(4), 38–49. DOI: https://doi.org/10.36023/ujrs.2024.11.4.276
6. Вересень 2024 – Атаки на енергетичну інфраструктуру України: шкода цивільному населенню / Моніторингова місія ООН з прав людини в Україні. URL: https://ukraine.ohchr.org/uk/Attacks-on-Ukraines-Energy-Infrastructure-Harm-to-the-Civilian-Population
7. Гапонов О.О. Особливості правового регулювання у сфері транспортної інфраструктури. *Право і суспільство*. №1/2024. Т.2. DOI https://doi.org/10.32842/2078-3736/2024.1.2.49
8. Гапонов О.О. Транспортна інфраструктура як ключовий фактор економічного зростання України. *Правові новели*, № 22/2024. DOI: https://doi.org/10.32782/ln.2024.22.38
9. Глосарій з гібридних загроз 2.0. 2024. URL: https://openarchive.nure.ua/entities/publication/c2051668-3a66-458a-97a2-7df51697b99e

10. Грані історії: зб. наук. праць. Спеціальний випуск: Домени гібридних загроз / автори упорядники: С. Гришко, М. Головянко, П. Худ, О. Карпенко, В. Яновська, А. Худолій, Т. Жовтенко, Т. Рева, Л. Величко, М. Білоконь, Г. Докашенко, В. Докашенко, В. Концур. Дніпро: Ліра, 2024. – Вип. 6 (14). – 100 с. DOI: https://doi.org/10.61655/2708-1249.6(14).2024.special-issue

11. Гречан А., Гавриков Д. Роль транспортного комплексу у забезпеченні сталого розвитку національної економіки. *Modeling the Development of the Economic Systems*, 2024, № 4, с. 138–144. DOI: DOI: https://doi.org/10.31891/mdes/2024-14-19

12. Гринь А., Толок П. Вплив транспортної інфраструктури на економічний розвиток регіонів, оцінка ефективності управління дорожнім господарством. *Вісник Хмельницького національного університету*. Серія: Економічні науки, 2024, № 334(5). DOI: https://doi.org/10.31891/2307-5740-2024-334-13

13. Зубок В.Ю., Давидюк А.В., Клименко Т.М. Кібербезпека критичної інфраструктури в законодавстві України та в директиві (ЄС) 2022/2555. *Electronic Modeling*. 2023. V. 45. № 5, с. 54-66. DOI: https://doi.org/10.15407/emodel.45.05.054

14. Кирчата І. М., Шершенюк О. М., Кирчатий Ю. В. Стратегічні орієнтири відновлення та розвитку транспортної інфраструктури: проєктний підхід. *Проблеми підвищення ефективності інфраструктури*. 2024. №1(32). С. 48–56. DOI: https://doi.org/10.30977/PPB.2226-8820.2024.32.48

15. Коли слова стали зброєю: безпрецедентні ризики для цивільного населення через поширення дезінформації. URL: https://civiliansinconflict.org/wp-content/uploads/2023/11/When-Words-Become-Weapons_UKR.pdf

16. Кресін О. Протидія гібридним загрозам в українському законодавстві. *Зовнішня торгівля: економіка, фінанси, право*. 2022. № 1. С. 4-17. DOI: https://doi.org/10.31617/zt.knute.2022(120)01

17. Міністерство розвитку громад та територій України. URL: https://mtu.gov.ua/content/hto-mi-e.html

18. Про внесення змін до Закону України «Про критичну інфраструктуру» щодо імплементації положень Директиви (ЄС) 2022/2557 Європейського парламенту та Ради від 14 грудня 2022 року про стійкість критично важливих об'єктів і скасування Директиви Ради 2008/114/ЕС. Проєкт закону України від 14.11.2024 р. № 12208. URL: https://ips.ligazakon.net/document/JI11915I

19. Про схвалення Національної транспортної стратегії України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках. Постанова від 27 грудня 2024 р. № 1550 / Кабінет міністрів України. URL: https://zakon.rada.gov.ua/laws/show/1550-2024-%D0%BF#Text

20. Про схвалення Стратегії підвищення рівня безпеки дорожнього руху в Україні на період до 2024 року. Розпорядження від 21 жовтня 2020 р. № 1360-р / Кабінет міністрів України. URL: https://zakon.rada.gov.ua/laws/show/1360-2020-%D1%80#Text

21. Устименко А. Транспортна інфраструктура: поняття та змістовне наповнення. *Актуальні проблеми правознавства*. 1 (37)/2024 DOI: https://doi.org/10.35774/app2024.01.131

22. Хронологія російсько-української війни: «гібридна» фаза (лютий 2014 – лютий 2022). Це варто пам'ятати / Івано-Франківська обласна державна адміністрація. URL: https://www.if.gov.ua/news/khronolohiia-rosiisko-ukrainskoi-viiny-hibrydna-faza-liutyi-2014-liutyi-2022-tse-varto-pamiataty

23. Целлєр В., Крамський С. Інфраструктурна підтримка інновацій в сфері транспортної логістики в умовах турбулентності під час війни. *Економіка та суспільство*. 2024. № 67. DOI: https://doi.org/10.32782/2524-0072/2024-67-142

24. Шрамко С.С. Оцінка сучасного стану безпеки дорожнього руху в Україні. *Вісник асоціації кримінального права України*. 2024. Том 2 № 22. DOI: https://doi.org/10.21564/2311-9640.2024.22.315949

Стаття надійшла до редакції 21.10.2024
Стаття рекомендована до друку 21.11.2024

Larysa Velychko, Doctor of Law, Professor, Head of the Law,
National Security and European Integration Chair, Educational and Scientific Institute
«Institute of Public Administration», V. N. Karazin Kharkiv National University, 4 Svobody Sq.,
Kharkiv, 61022, Ukraine
ORCID ID: https://orcid.org/0000-0003-3029-4719 e-mail: Velychkolara71@gmail.com

Mykhailo Bilokon, PhD in Public Administration, Associate Professor of Law,
National Security and European Integration Chair, Educational and Scientific Institute
«Institute of Public Administration», V. N. Karazin Kharkiv National University, 4 Svobody Sq.,
Kharkiv, 61022, Ukraine
ORCID ID: https://orcid.org/0000-0002-5389-7013 e-mail: m.bilokon@karazin.ua

HYBRID THREATS TO TRANSPORT INFRASTRUCTURE: CHALLENGES FOR STATE REGULATION AND NATIONAL SECURITY

Abstract. In the context of modern global challenges, transport infrastructure plays a strategic role in ensuring economic stability, population mobility, effective functioning of supply chains and the state's defense capability. At the same time, it becomes a target for hybrid threats that combine cyberattacks, physical sabotage, information manipulation and economic pressure. This problem is of particular importance for Ukraine, which has been in an active hybrid confrontation for more than a decade. Military actions aimed at destroying critical infrastructure, massive cyberattacks on transport networks, as well as external economic pressure create a complex challenge for the system of state regulation and ensuring national security.

The relevance of the study is due to the need to develop effective mechanisms of state policy aimed at increasing the resilience of transport infrastructure to new threats. Today, the destruction or incapacitation of key transport nodes can not only cause significant economic losses, but also cause social instability, disrupt the supply of critical resources, complicate military logistics and reduce the level of international trade. At the same time, foreign experience shows that the integration of preventive measures, modern threat monitoring technologies, cyber defense and information security allows minimizing the impact of hybrid attacks on the transport system.

The article provides a comprehensive analysis of the main types of hybrid threats that affect transport infrastructure, including: cyberattacks on automated transport management systems, physical sabotage against strategic facilities (bridges, railway junctions, airports, seaports), economic pressure (sanctions, blocking of transport corridors) and information and psychological operations (disinformation about the safety of transport routes, creating panic, undermining trust in state institutions in the transport sector).

The results of the study show that hybrid threats are systemic in nature and require a comprehensive response from the state. An assessment of the current state of security of

Ukraine's transport infrastructure was conducted, its main vulnerabilities were identified, including insufficient coordination between state and private entities in the field of transport security, the obsolescence of part of the regulatory framework, limited capabilities for crisis response to large-scale threats. A conceptual model of the state regulation strategy was proposed, which includes the adaptation of Ukrainian legislation to EU standards and NATO practices, strengthening interdepartmental coordination, developing cybersecurity of critical transport facilities, integrating modern threat monitoring technologies, and implementing rapid response crisis centers.

Special attention is paid to the analysis of international experience in protecting transport infrastructure from hybrid threats, including the strategies of the European Union, the United States and NATO countries to ensure transport security. The feasibility of implementing best international practices in Ukraine is substantiated, in particular, the creation of a state system of cyber protection of the transport industry, the expansion of public-private partnerships in the field of transport hub security and the involvement of international technical assistance for the modernization of critical infrastructure.

The proposed measures include the creation of a nationwide transport security monitoring system, the implementation of the latest cybersecurity standards, the integration of artificial intelligence technologies to identify potential threats, and the development of international cooperation mechanisms to minimize external threats. Prospects for further scientific research in the field of strategic transport security management, risk analysis, and the implementation of new technological solutions for the protection of critical infrastructure are outlined.

Keywords: *transport infrastructure; national security; critical infrastructure; sustainability of transport systems; logistics security; regional level; national infrastructure; railway transport.*

In cites: Velychko, L. Yu., & Bilokon, M. Yu. (2024). Hybrid threats to transport infrastructure: challenges for state regulation and national security. *Theory and Practice of Public Administration*, 2 (79), 442–464. http://doi.org/10.26565/1727-6667-2024-2-23 [in Ukrainian].

REFERENCES:

1. Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2021). A Review of Colonial Pipeline Ransomware Attack. URL: https://ieeexplore.ieee.org/abstract/document/10181159/authors#authors (accessed 09 February 2025).

2. Malik, Z. A., Butt, M. M., Xing, H. M., Nazir, B., Shabbir, S., Fatima, H., Khan, A. U., & Zheng, M. (2022). Cyber Warfare from Pakistan-India: A Critical Analysis. *International Journal of Special Education*, 37(3). URL: https://www.researchgate.net/profile/Sundas-Malik/publication/373737800_Cyber_Warfare_from_Pakistan-India_A_Critical_Analysis/links/64fa10dfe098013a83decaa6/Cyber-Warfare-from-Pakistan-India-A-Critical-Analysis.pdf

3. Schwarz, M., Marx, M., & Federrath, H. (2021). A Structured Analysis of Information Security Incidents in the Maritime Sector. DOI: https://doi.org/10.48550/arXiv.2112.06545

4. The Ukrainian Power Grid Was Hacked Again. URL: https://web.archive.org/web/20170118201525/http://motherboard.vice.com/read/ukrainian-power-station-hacking-december-2016-report

5. Borovyk, K. V., Gapon, S. V., Pyshnohraiiev, I. O., & Khashchevatska, A. I. (2024). Modeling the Suitability of Territories for the Placement of Critical Infrastructure of Ukraine

under Military Threats. *Ukrainian Journal of Remote Sensing*, 11(4), 38–49. DOI: https://doi.org/10.36023/ujrs.2024.11.4.276

6. September 2024 – Attacks on Ukraine's energy infrastructure: harm to civilians / UN Human Rights Monitoring Mission in Ukraine. URL: https://ukraine.ohchr.org/uk/Attacks-on-Ukraines-Energy-Infrastructure-Harm-to-the-Civilian-Population [in Ukrainian].

7. Haponov, O. O. (2024). Features of Legal Regulation in the Field of Transport Infrastructure. *Law and Society*, 1(2). DOI: https://doi.org/10.32842/2078-3736/2024.1.2.49 [in Ukrainian].

8. Haponov, O. O. (2024). Transport Infrastructure as a Key Factor in Ukraine's Economic Growth. *Legal Novels*, 22. DOI: https://doi.org/10.32782/ln.2024.22.38 [in Ukrainian].

9. Hybrid Threats Glossary 2.0. (2024). Retrieved from: https://openarchive.nure.ua/entities/publication/c2051668-3a66-458a-97a2-7df51697b99e [in Ukrainian].

10. Hryshko, S., Holovian, M., Khud, P., Karpenko, O., Yanovska, V., Khudolii, A., Zhovtenko, T., Reva, T., Velychko, L., Bilokon, M., Dokashenko, H., Dokashenko, V., & Kontsur, V. (2024). Facets of History: Collection of Scientific Papers. Special Issue: Domains of Hybrid Threats. Dnipro: Lira, 6(14), 100. DOI: https://doi.org/10.61655/2708-1249.6(14).2024.special-issue [in Ukrainian].

11. Grechan, A., & Havrykov, D. (2024). The Role of the Transport Complex in Ensuring Sustainable Development of the National Economy. *Modeling the Development of the Economic Systems*, 4, 138–144. DOI: https://doi.org/10.31891/mdes/2024-14-19 [in Ukrainian].

12. Hryn, A., & Tolok, P. (2024). The Impact of Transport Infrastructure on Regional Economic Development: Assessing Road Management Efficiency. *Bulletin of Khmelnytskyi National University*. Economic Sciences Series, 334(5). DOI: https://doi.org/10.31891/2307-5740-2024-334-13 [in Ukrainian].

13. Zubok, V. Y., Davydiuk, A. V., & Klymenko, T. M. (2023). Cybersecurity of Critical Infrastructure in Ukrainian Legislation and Directive (EU) 2022/2555. *Electronic Modeling*, 45(5), 54-66. DOI: https://doi.org/10.15407/emodel.45.05.054 [in Ukrainian].

14. Kyrchata, I. M., Shersheniuk, O. M., & Kyrchatyi, Y. V. (2024). Strategic Guidelines for the Restoration and Development of Transport Infrastructure: Project-Based Approach. *Problems of Increasing the Efficiency of Infrastructure*, 1(32), 48–56. DOI: https://doi.org/10.30977/PPB.2226-8820.2024.32.48 [in Ukrainian]

15. When words became weapons: unprecedented risks to civilians due to the spread of disinformation. URL: https://civiliansinconflict.org/wp-content/uploads/2023/11/When-Words-Become-Weapons_UKR.pdf [in Ukrainian].

16. Kresin, O. (2022). Countering Hybrid Threats in Ukrainian Legislation. *Foreign Trade: Economics, Finance, Law*, 1, 4-17. DOI: https://doi.org/10.31617/zt.knute.2022(120)01 [in Ukrainian].

17. Ministry of Community and Territorial Development of Ukraine. URL: https://mtu.gov.ua/content/hto-mi-e.html [in Ukrainian].

18. On Amendments to the Law of Ukraine «On Critical Infrastructure» Regarding the Implementation of the Provisions of Directive (EU) 2022/2557 of the European Parliament and the Council of 14 December 2022. Draft Law of Ukraine No. 12208 (2024). URL: https://ips.ligazakon.net/document/JI11915I [in Ukrainian].

19. On Approval of the National Transport Strategy of Ukraine until 2030 and the Operational Plan for Its Implementation in 2025-2027. Resolution No. 1550. Cabinet of Ministers of Ukraine. (2024). URL: https://zakon.rada.gov.ua/laws/show/1550-2024-%D0%BF#Text [in Ukrainian].

20. On Approval of the Strategy for Increasing Road Traffic Safety in Ukraine until 2024. Order No. 1360-r. Cabinet of Ministers of Ukraine. (2020). URL: https://zakon.rada.gov.ua/laws/show/1360-2020-%D1%80#Text [in Ukrainian].

21. Ustymenko, A. (2024). Transport Infrastructure: Concept and Content. *Current Problems of Law*, 1(37). DOI: https://doi.org/10.35774/app2024.01.131 [in Ukrainian]).

22. Chronology of the Russian-Ukrainian war: the «hybrid» phase (February 2014 – February 2022). It is worth remembering / Ivano-Frankivsk Regional State Administration. URL: https://www.if.gov.ua/news/khronolohiia-rosiisko-ukrainskoi-viiny-hibrydna-faza-liutyi-2014-liutyi-2022-tse-varto-pamiataty [in Ukrainian].

23. Tselier, V., & Kramskyi, S. (2024). Infrastructure Support for Innovations in Transport Logistics During Turbulence in Wartime. *Economy and Society*, 67. DOI: https://doi.org/10.32782/2524-0072/2024-67-142 [in Ukrainian].

24. Shramko, S. S. (2024). Assessment of the Current State of Road Traffic Safety in Ukraine. *Bulletin of the Association of Criminal Law of Ukraine*, 2(22). DOI: https://doi.org/10.21564/2311-9640.2024.22.315949 [in Ukrainian].

The article was received by the editors 21.10.2024
The article is recommended for printing 21.11.2024