УДК 343.3/.7:351.862.6
DOI https://doi.org/10.32782/2524-0374/2024-7/96

ЗАСАДИ МІЖНАРОДНОЇ КРИМІНАЛЬНО-ПРАВОЇ ПОЛІТИКИ ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

PRINCIPLES OF INTERNATIONAL CRIMINAL LAW POLICY TO COUNTERACT CRIMINAL OFFENSES AT CRITICAL INFRASTRUCTURE

Герасименко О.М., к.ю.н.,
докторант
Національна академія Служби безпеки України

Стаття присвячена аналізу міжнародних правових засад кримінально-правової політики протидії кримінальним правопорушенням на об'єктах критичної інфраструктури. У сучасному світі критична інфраструктура відіграє ключову роль у забезпеченні стабільного функціонування суспільства та держави, включаючи енергетичні мережі, транспортні системи, водопостачання, зв'язок та інформаційні системи, медичні установи та інші важливі елементи.

У статті розглядаються основні міжнародні документи, які регулюють питання протидії окремим кримінальним правопорушенням на об'єктах критичної інфраструктури, надаючи всебічний аналіз їх змісту та практичної імплементації. Зокрема, значну увагу приділено Резолюції Ради Безпеки ООН 1373 (2001), яка стала ключовим інструментом у глобальній боротьбі з тероризмом, встановлюючи норми щодо криміналізації підтримки терористичних груп і забезпечення безпеки критичних об'єктів. Також детально аналізується Конвенція ООН про боротьбу з фінансуванням тероризму (1999), яка зобов'язує держави приймати заходи для запобігання фінансуванню терористичних актів, що є важливим для захисту об'єктів критичної інфраструктури від можливих атак.

Висвітлюються ключові аспекти міжнародного співробітництва, зокрема, координація зусиль між державами, що є необхідною для ефективної протидії загрозам. Обмін інформацією та досвідом між різними країнами дозволяє швидше та ефективніше виявляти та реагувати на потенційні загрози, що стосуються критичних об'єктів. Спільні заходи з запобігання включають розробку стандартизованих процедур та практик, що забезпечують виявлення та нейтралізацію загроз до їх реалізації. Міжнародні організації та угоди створюють платформу для такої співпраці, сприяючи встановленню єдиних підходів та обміну найкращими практиками між державами, що є ключовими елементами у забезпеченні безпеки критичної інфраструктури на глобальному рівні.

Увагу приділено питанням кібербезпеки, що стає все більш актуальним у зв'язку з розвитком сучасних технологій. Аналізуються документи та дослідження, спрямовані на боротьбу з кібертероризмом та забезпечення кіберстійкості критичної інфраструктури. Також розглядаються питання фізичної безпеки ядерних об'єктів, зокрема, в рамках Конвенції про фізичний захист ядерного матеріалу і ядерних установок (1980) та її поправок 2005 року. Законодавчі ініціативи України, такі як Закон «Про критичну інфраструктуру» від 16 листопада 2021 року, розглядаються у контексті їх відповідності міжнародним стандартам та необхідності вдосконалення національних механізмів захисту.

Ключові слова: критична інфраструктура, кримінальні правопорушення, міжнародне право, кібербезпека, тероризм, організована злочинність, міжнародне співробітництво.

The article is devoted to the analysis of the international legal foundations of the criminal legal policy to counteract criminal offenses at the objects of critical infrastructure. In today's world, critical infrastructure plays a key role in ensuring the stable functioning of society and the state, including energy networks, transport systems, water supply, communications and information systems, medical institutions and other important elements.

The article examines the main international documents that regulate the issues of combating individual criminal offenses at critical infrastructure facilities, providing a comprehensive analysis of their content and practical implementation. In particular, considerable attention is paid to UN Security Council Resolution 1373 (2001), which has become a key tool in the global fight against terrorism, establishing norms for criminalizing support for terrorist groups and ensuring the security of critical facilities. The UN Convention against the Financing of Terrorism (1999), which obliges states to take measures to prevent the financing of terrorist acts, is important for protecting critical infrastructure from possible attacks, is also analyzed in detail.

Highlights key aspects of international cooperation, in particular, coordination of efforts between states, which is necessary to effectively counter threats. The exchange of information and experience between different countries allows faster and more effective detection and response to potential threats related to critical objects. Joint prevention measures include the development of standardized procedures and practices to ensure that threats are identified and neutralized before they are implemented. International organizations and agreements create a platform for such cooperation, contributing to the establishment of common approaches and the exchange of best practices between states, which are key elements in ensuring the security of critical infrastructure at the global level.

Attention is paid to cybersecurity issues, which is becoming increasingly relevant in connection with the development of modern technologies. Documents and research aimed at combating cyber terrorism and ensuring the cyber stability of critical infrastructure are analyzed. The physical security of nuclear facilities is also considered, in particular, under the Convention on the Physical Protection of Nuclear Material and Nuclear Installations (1980) and its 2005 amendments. Legislative initiatives of Ukraine, such as the Law "On Critical Infrastructure" of November 16, 2021, are considered in the context of their compliance with international standards and the need to improve national protection mechanisms.

Key words: critical infrastructure, criminal offenses, international law, cybersecurity, terrorism, organized crime, international cooperation.

Постановка проблеми. У світі критична інфраструктура відіграє ключову роль у забезпеченні стабільного функціонування суспільства та держави. Об'єкти критичної інфраструктури включають енергетичні мережі, транспортні системи, водопостачання, зв'язок та інформаційні системи, медичні установи, а також інші важливі для життєдіяльності елементи. Їх надійна робота є основою національної безпеки та суспільного добробуту. Однак ці об'єкти стають все більш вразливими до різних загроз, зокрема кримінальних правопорушень.

Кримінальні правопорушення на об'єктах критичної інфраструктури створюють реальну загрозу національній безпеці, включаючи порушення життєво важливих послуг, економічні збитки та загрозу життю та здоров'ю громадян України. В умовах глобалізації та зростання складності сучасних технологій виникає нагальна потреба в розробці та впровадженні ефективних кримінально-правових механізмів протидії таким правопорушенням.

У цьому контексті міжнародно-правові засади політики протидії кримінальним правопорушенням на об'єктах критичної інфраструктури набувають особливого значення. З одного боку, міжнародні норми та стандарти сприяють уніфікації підходів до захисту критичної інфраструктури, забезпечуючи узгодженість та координа-

цію зусиль різних держав. З іншого боку, розвиток міжнародного права дозволяє враховувати специфіку різних регіонів та держав, адаптуючи загальні принципи до національних умов, зокрема українських національних в умовах повномасштабної війни з рф.

У даній статті досліджуються основні міжнародні засади міжнародно-правові політики протидії кримінальним правопорушенням на об'єктах критичної інфраструктури, що, зі свого боку, є правовою рамкою для національного законодавця в Україні. Аналізуються ключові міжнародні документи, що регулюють цю сферу, а також практичні аспекти їх імплементації на національному рівні. Приділяється увага питанням співпраці та координації між державами у забезпеченні безпеки сфери критичної інфраструктури, а також ролі міжнародних організацій у цьому процесі.

Зважаючи на значущість означеного назвою статті предмета дослідження для національної безпеки, його дискусійність, а також з огляду сучасних потреб теорії та практики, вбачається актуальним проведення фахового дослідження.

Аналіз останніх досліджень і публікацій. Умовою розвитку вітчизняних нормативно-правових засад протидії кримінальним правопорушенням на об’єктах критичної інфраструктури є правова взаємодія на міжнародному рівні та адаптація національного законодавства положенням міжнародних норм. Розв’язання цієї проблеми на науковому рівні присвячені роботи вітчизняних вчених.

Так, І. В. Гора у своєму дослідженні розглянула проблеми діяльності Служби безпеки України (далі по тексту – СБ України) з протидії тероризму. Серед інших питань автором розкрито оперативно-розшукові, контррозвідувальні, кримінальні процесуальні та криміналістичні аспекти діяльності органів СБ України в боротьбі зі злочинами терористичної спрямованості. Надано загальну характеристику тероризму та його видів, розкрито поняття, сутність, міжнародні аспекти кримінально-правової політики протидії тероризму. Науковиця акцентує увагу на необхідності вивчення досвіду окремих країн ЄС, Великої Британії та США у сфері антитерористичної діяльності. Робиться висновок про те, що неабияке значення мають сьогодні питання розробки окремих законодавчих актів стосовно превентивних заходів реагування на реальну терористичну загрозу, з визначенням місця й ролі в антитерористичній діяльності СБ України [1, с. 168].

За загальною редакцією В. А. Колесника досліджено загальнотеоретичні й окремі практичні проблеми протидії зочинам, що посягають на інформаційну безпеку держави. Автором визначається місце інформаційної безпеки в системі національної та державної безпеки України, її поняття й сутність забезпечення правоохоронними органами та спецслужбами. Розкрито кримінологічні, кримінально-правові та криміналістичні питання вчинення, класифікації, виявлення й досудового розслідування злочинів у сфері інформаційної безпеки держави та кіберзлочинів як їхньої складової. Приділено увагу правовій основі, закордонному досвіду та діяльності оперативних і слідчих підрозділів СБ України з протидії злочинам проти інформаційної безпеки, актуальним питанням досудового розслідування злочинів дослідженої категорії, зокрема організаційно-тактичним, методичним аспектам і використанню слідчим, прокурором можливостей судової експертизи. Науковець робить висновок, що все більшої практичної значущості набуває позитивний досвід окремих європейських країн, США, а також окремих країн пострадянського простору, яким вдалося не тільки належним чином організувати роботу власних спецслужб і правоохоронних інституцій, а й досягти позитивних зрушень у питаннях протидії інформаційним злочинам, що посягають на безпеку державних інтересів кожної із цих країн [2, с. 241].

У дослідженні С. Є. Кучерини та Д. О. Олєйнікова аналізуються сучасні виклики кримінально-правової охорони об’єктів критичної інфраструктури, підкреслюючи необхідність вдосконалення законодавчої бази та розвитку міжнародного співробітництва для ефективної протидії загрозам [3, с. 90–98]. Важливість цих питань підкріплюється Д. Распутнім, який розглядає практичні аспекти розслідування злочинів проти критичної інфраструктури в умовах війни, зокрема методи криміналістики та специфіку воєнного стану [4, с. 151–154].

О. О. Юріков вносить свій внесок у цей дискурс, аналізуючи питання кримінальної відповідальності за умисне пошкодження або руйнування телекомунікаційних мереж. Юріков підкреслює значущість правового врегулювання таких злочинів та необхідність посилення відповідальності для забезпечення належного захисту об’єктів інфраструктури [5, с. 123–127]. Цей погляд підтримують С. Є. Кучерина та Д. О. Олєйніков, які досліджують проблемні аспекти впровадження кримінальної відповідальності за кібертероризм, підкреслюючи необхідність адаптації законодавства до сучасних кіберзагроз [6, с. 70–81].

І. Р. Шинкаренко та В. П. Захаров у своєму дослідженні акцентують на убезпеченні об’єктів та суб’єктів інфраструктури авіаційно-космічної галузі України. Вони підкреслюють важливість інтеграції міжнародних стандартів безпеки та створення національних механізмів захисту [7, с. 59–68]. Завершує цей огляд М. Гуцалюк, який аналізує стратегії протидії сучасним кіберзагрозам та забезпечення кіберстійкості критичної інфраструктури України, акцентуючи на важливості розвитку національних можливостей кіберзахисту та міжнародного співробітництва [8, с. 164–177].

Разом ці дослідження забезпечують комплексне бачення захисту критичної інфраструктури, акцентуючи на необхідності вдосконалення законодавства, розвитку національних та міжнародних механізмів співробітництва, а також на важливості інтеграції сучасних технологій і методологій для ефективного захисту від різних видів загроз. Тим часом, міжнародно-правові аспекти захисту об’єктів критичної інфраструктури від злочинів досі залишаються малодослідженими, що підкреслює актуальність обраної нами тематики.

Формулювання цілей. Метою статті є аналіз міжнародних кримінально-правових засад політики протидії кримінальним правопорушенням на об'єктах критичної інфраструктури, а також розробка рекомендацій щодо підвищення ефективності цих заходів на національному рівні.

Виклад основного матеріалу. Згідно із Законом України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX [22], об'єкти критичної інфраструктури (далі по тексту – ОКІ) визначаються як об'єкти, їх частини та сукупності, які є важливими для економіки, національної безпеки та оборони. Порушення функціонування таких об'єктів може завдати значної шкоди життєво важливим національним інтересам. Ці об'єкти забезпечують життєво важливі функції та/або послуги, збої в наданні яких призводять до швидких негативних наслідків для національної безпеки.

Безпека критичної інфраструктури прирівнюється до стану захищеності критичної інфраструктури, за якого забезпечується її функціональність, безперервність роботи, відновлюваність, цілісність і стійкість. Життєво важливі функції та/або послуги – це функції та/або послуги, реалізація яких забезпечується органами державної влади, установами, суб’єктами господарювання та організаціями будь-якої форми власності. Порушення надання таких послуг призводить до швидких негативних наслідків для національної безпеки. Захист критичної інфраструктури охоплює всі види діяльності, що виконуються для своєчасного виявлення, запобігання і нейтралізації

загроз безпеці об’єктів критичної інфраструктури, а також мінімізації та ліквідації наслідків у разі їх реалізації.

До критичної інфраструктури належать об'єкти, віднесення яких до категорії критичних здійснюється за сукупністю критеріїв, визначених їх соціальною, політичною, економічною, екологічною значущістю для забезпечення оборони країни, безпеки громадян, суспільства, держави та правопорядку. Це можуть бути енергетичні мережі, транспортні системи, водопостачання, зв'язок та інформаційні системи, медичні установи та інші важливі для життєдіяльності елементи. Віднесення об’єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України.

Враховуючи зазначене можемо зробити поточний висновок, що об'єкти критичної інфраструктури є ключовими для національної безпеки й сталого функціонування держави та суспільства України, а протидія кримінальним правопорушенням займає важливе місце в міжнародно-правовій політиці. Нижче ми проаналізуємо основні джерела міжнародного права з означеного предмета регулювання.

Так, Міжнародна конвенція про боротьбу з фінансуванням тероризму (1999) [20] визначає, що фінансування тероризму є одним з основних механізмів здійснення терористичних актів. Згідно зі статтею 2, держави-учасниці зобов'язані криміналізувати умисне надання або збирання коштів з наміром використання їх для здійснення терористичних актів. Захист об'єктів критичної інфраструктури забезпечується через виявлення та блокування фінансових потоків, які можуть бути спрямовані на організацію атак на ці об'єкти. У цьому контексті важливою є співпраця між фінансовими установами та органами безпеки для моніторингу та запобігання підозрілим фінансовим операціям.

З іншого боку, Конвенція ООН проти транснаціональної організованої злочинності (2000) [21] розглядає організовану злочинність як загрозу, що може включати атаки на критичну інфраструктуру. У статті 5 конвенції підкреслюється важливість криміналізації участі в організованій злочинній групі. Цей документ наголошує на важливості міжнародного співробітництва у сфері правосуддя, включаючи екстрадицію та взаємну правову допомогу. Захист критичної інфраструктури в цьому контексті полягає у створенні міжнародних механізмів для боротьби з організованими злочинними угрупованнями, що можуть намагатися атакувати такі об'єкти з метою дестабілізації.

Міжнародна конвенція про боротьбу з бомбовим тероризмом (1997) [10] зосереджується на запобіганні використанню вибухових пристроїв для терористичних атак. Стаття 2 конвенції зобов'язує держави криміналізувати незаконне та умисне зберігання, виготовлення, транспортування або використання вибухових речовин з метою вчинення терористичного акту. Конвенція також передбачає заходи для безпеки об'єктів критичної інфраструктури, включаючи встановлення стандартів безпеки та проведення регулярних перевірок. Важливим аспектом є координація між правоохоронними органами та операторами критичної інфраструктури для забезпечення своєчасного виявлення та запобігання терористичним загрозам.

Далі, Конвенція ООН про ядерну безпеку (1994) [12] встановлює міжнародні стандарти для забезпечення безпеки ядерних установок. Стаття 6 цієї конвенції зобов'язує держави-учасниці створити та підтримувати правову та регуляторну базу для забезпечення безпеки ядерних установок, включаючи регулярні перевірки та оцінки ризиків. У контексті захисту об'єктів критичної інфраструктури, ця конвенція звертає увагу на необхідності забезпечення фізичного захисту ядерних матеріалів і установок від терористичних атак. Міжнародна співпраця в рамках цієї конвенції дозволяє державам обмінюватися досвідом та найкращими практиками для підвищення безпеки.

Міжнародна конвенція про боротьбу з актами ядерного тероризму (2005) [13] доповнює Конвенцію про ядерну безпеку, зосереджуючись на попередженні, виявленні та покаранні за акти ядерного тероризму. Стаття 2 цієї конвенції передбачає криміналізацію будь-яких актів, пов'язаних з ядерним тероризмом, таких як виготовлення, володіння або використання ядерних матеріалів з метою заподіяння шкоди. Конвенція підкреслює важливість міжнародного співробітництва, зокрема обмін інформацією та координацію зусиль правоохоронних органів. Це дозволяє країнам ефективніше захищати свої об'єкти критичної інфраструктури від ядерних загроз.

Конвенція про фізичний захист ядерного матеріалу і ядерних установок (1980, поправки 2005) [14] є ще одним важливим документом у сфері забезпечення безпеки ядерних об'єктів. Вона встановлює стандарти фізичного захисту ядерних матеріалів під час їх використання, зберігання та транспортування. Поправки до конвенції, прийняті у 2005 році, розширюють її сферу дії, включаючи захист ядерних установок від актів саботажу. Стаття 5 конвенції зобов'язує держави впроваджувати ефективні заходи для запобігання, виявлення та реагування на спроби незаконного вилучення або пошкодження ядерних матеріалів і установок.

Резолюція Ради Безпеки ООН 1373 (2001) [15] була прийнята одразу після терористичних атак 11 вересня 2001 року і стала важливим кроком у міжнародній боротьбі з тероризмом. Ця резолюція зобов'язує держави вживати широкого спектра заходів для запобігання тероризму, включаючи криміналізацію фінансування терористичних актів, заморожування фінансових активів терористів, заборону надання будь-якої форми підтримки терористичним групам і активну співпрацю у сфері обміну інформацією. Зокрема, у статті 1(c) резолюції наголошується на необхідності співпраці між державами для попередження атак на критичну інфраструктуру.

Резолюція Ради Безпеки ООН 1540 (2004) [16] спрямована на запобігання розповсюдженню зброї масового знищення і терористичних актів, пов'язаних з нею. Вона зобов'язує держави створити внутрішньодержавний контроль, щоб запобігти потраплянню ядерних, хімічних та біологічних матеріалів до рук терористів. У статті 3 резолюції підкреслюється важливість вжиття заходів для забезпечення фізичного захисту таких матеріалів та пов'язаних з ними об'єктів критичної інфраструктури. Резолюція також звертає увагу на важливості міжнародного співробітництва і технічної допомоги для посилення національних можливостей захисту.

Рамкова Конвенція Ради Європи про боротьбу з тероризмом (2005) [17] має на меті покращити співпрацю між європейськими країнами у боротьбі з тероризмом. Конвенція визначає обов'язки держав у криміналізації терористичних актів, включаючи ті, що спрямовані на об'єкти критичної інфраструктури, та забезпечує екстрадицію підозрюваних у терористичній діяльності. Стаття 4 конвенції підкреслює важливість запобігання терористичним актам через обмін інформацією та досвідом між державами-учасницями, а також координацію зусиль у забезпеченні безпеки критичних об'єктів.

Резолюція 1373 закладає основу для глобальної співпраці у протидії тероризму, акцентуючи на необхідності криміналізації підтримки терористів. Резолюція 1540 зосереджується на запобіганні використанню зброї масового знищення, що включає фізичний захист об'єктів критичної інфраструктури. Рамкова Конвенція Ради Європи про боротьбу з тероризмом забезпечує правові рамки для співпраці та обміну інформацією між європейськими країнами для захисту від терористичних загроз. Ці документи взаємодоповнюють один одного, створюючи ефективну систему захисту критичних об'єктів на міжнародному рівні.

Проведений аналіз зазначених вище норм показує, як міжнародна спільнота реагує на загрози вчинення кримінальних правопорушень і працює над створенням комплексних механізмів для захисту критичної інфраструктури.

Глобальна стратегія ООН з протидії тероризму (2006) [18] є комплексним документом, що містить низку заходів для боротьби з тероризмом на міжнародному рівні. Стратегія підкреслює важливість координації між державами для попередження терористичних актів, особливо щодо захисту об'єктів критичної інфраструктури. Зокрема, стратегія акцентує на необхідності зміцнення державних можливостей у захисті критичної інфраструктури від терористичних загроз шляхом обміну інформацією, підвищення стандартів безпеки та спільних навчань.

Директива Європейського Парламенту та Ради 2008/114/ЕС про ідентифікацію та позначення європейських критичних інфраструктур та оцінку потреб щодо їх захисту спрямована на підвищення захисту критичної інфраструктури в Європейському Союзі [19]. Цей документ встановлює процедури для ідентифікації критичних інфраструктур, визначає їх важливість для безпеки держав-членів та вводить заходи для зниження ризиків. Директива вимагає від держав-членів розробити національні програми захисту, що включають співпрацю між публічним і приватним секторами.

Ці міжнародні документи підкреслюють важливість координації та співпраці між державами для захисту критичної інфраструктури. Глобальна стратегія ООН з протидії тероризму акцентує на всебічному підході до боротьби з тероризмом, включаючи зміцнення захисту критичних об'єктів. Директива ЄС 2008/114/ЕС забезпечує конкретні процедури для ідентифікації та захисту критичних інфраструктур в Європі, тоді як Конвенція про фізичний захист ядерного матеріалу і ядерних установок встановлює стандарти безпеки для ядерних об'єктів.

Зазначені вище документи взаємодоповнюють один одного, створюючи комплексну міжнародну правову базу для захисту критичних об'єктів від терористичних загроз. Вони сприяють зміцненню національних систем безпеки, підвищенню рівня міжнародного співробітництва та обміну інформацією, що є ключовими елементами для забезпечення глобальної безпеки.

Висновки. У контексті розгляду міжнародних правових засад політики протидії кримінальним правопорушенням на об'єктах критичної інфраструктури, стає очевидним, що це питання набуває все більшої актуальності та складності. На підставі проведеного аналізу міжнародних документів та практичних аспектів їх імплементації можна зробити кілька ключових висновків.

По-перше, міжнародна спільнота активно реагує на загрози, пов'язані з тероризмом та організованою злочинністю, що спрямовані на критичну інфраструктуру. Такі документи, як Резолюція Ради Безпеки ООН 1373 (2001), Конвенція ООН про боротьбу з фінансуванням тероризму (1999), та Директива Європейського Парламенту та Ради 2008/114/ЕС, створюють правову основу для координації зусиль різних держав у цій сфері. Це дозволяє уніфікувати підходи до захисту критичної інфраструктури, сприяючи узгодженості та ефективній співпраці на міжнародному рівні.

По-друге, важливість міжнародного співробітництва не обмежується лише обміном інформацією та досвідом. Вона включає створення спільних механізмів для запобігання, виявлення та реагування на загрози. Наприклад, Конвенція про фізичний захист ядерного матеріалу і ядерних установок (1980) та її поправки 2005 року встановлюють стандарти безпеки для ядерних об'єктів, що передбачають регулярні перевірки та оцінки ризиків. Це дозволяє державам обмінюватися найкращими практиками та підвищувати рівень безпеки на національному рівні.

По-третє, глобалізація та розвиток сучасних технологій створюють нові виклики для захисту від загроз критичної інфраструктури. Кіберзагрози стають складнішими та багатогранними, що вимагає постійного вдосконалення законодавства та розробки нових тактик та стратегій протидії. У цьому контексті важливу роль відіграють документи, що спрямовані на боротьбу з кібертероризмом, такі як Конвенція Ради Європи про кіберзлочинність (2001) [9].

Нарешті, національні кримінально-правової засади протидії кримінальним правопорушенням на об'єктах критичної інфраструктури мають бути адаптовані до міжнародних стандартів та норм. Це вимагає не лише законодавчих змін, але й впровадження ефективних практичних заходів, включаючи навчання, технічну підтримку та розвиток інституційних спроможностей. Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року є важливим кроком у цьому напрямку, визначаючи основні принципи та критерії захисту об'єктів критичної інфраструктури на національному рівні.

Таким чином, міжнародні кримінально-правові засади захисту об'єктів критичної інфраструктури закладають підстави для комплексного підходу протидії терористичним загрозам, що включає як уніфікацію міжнародних зусиль, так і адаптацію національних механізмів до сучасних викликів та загроз. Це дозволяє забезпечити стійкість та надійність критичної інфраструктури, що є основою національної безпеки та суспільного добробуту.

Отримані результати можуть послугувати підставою для розробки нового національного нормативно-правового регулювання протидії злочинам на об’єктах критичної інфраструктури, диференціації кримінальної відповідальності за їх вчинення та подальших наукових досліджень за цим напрямом.

ЛІТЕРАТУРА

1. Гора І.В. Діяльність Служби безпеки України з протидії тероризму: оперативні, процесуальні та криміналістичні аспекти : монографія. Київ, 2022. 540 с.

2. Колесник В.А. Злочини проти інформаційної безпеки держави: поняття, виявлення, досудове розслідування: монографія. за заг. ред. В.А. Колесника. Київ, 2023. 512 с.

3. Кучерина, С. Є., Олєйніков, Д. О. Сучасний стан кримінально-правової охорони об’єктів критичної інфраструктури. *Інформація і право*. 2021. № 1(36). С. 90-98.

4. Распутній Д. Особливості розслідування кримінальних правопорушень проти об’єктів повітряного транспорту в умовах воєнного стану. Актуальні проблеми та перспективи розвитку юридичної науки, освіти та технологій у XXI столітті в дослідженнях молодих учених. Харків, 2023. С. 151-154.

5. Юріков, О. О. Аналіз сучасного стану наукової розробленості питань кримінальної відповідальності за умисне пошкодження або руйнування телекомунікаційної мережі. *Juris Europensis Scientia*. 2021. № 3. С. 123-127.

6. Кучерина, С., Олєйніков, Д. Проблемні аспекти впровадження кримінальної відповідальності за кібертероризм. *Геополітика України: історія і сучасність*. 2021. № 1(26). С. 70-81.

7. Шинкаренко, І. Р., Захаров, В. П. Питання убезпечення об’єктів та суб’єктів інфраструктури авіаційно-космічної галузі України. *Пропілеї права та безпеки*. 2022. № 1. С. 59-68.

8. Гуцалюк, М. Стратегії протидії сучасним кіберзагрозам та забезпечення кіберстійкості критичної інфраструктури України. *Інформація і право*. 2024. № 2(49). С. 164-177.

9. Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), 2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата звернення: 31.07.2024).

10. Міжнародна конвенція про боротьбу з бомбовим тероризмом, 1997. URL: https://www.un.org/law/cod/finterr.htm (дата звернення: 31.07.2024).
11. Конвенція ООН проти корупції, 2003. URL: https://www.unodc.org/unodc/en/corruption/uncac.html (дата звернення: 31.07.2024).
12. Конвенція ООН про ядерну безпеку, 1994. URL: https://www.iaea.org/publications/documents/infcircs/convention-on-nuclear-safety (дата звернення: 31.07.2024).
13. Міжнародна конвенція про боротьбу з актами ядерного тероризму, 2005. URL: https://www.un.org/en/sc/ctc/docs/conventions/Conv13.pdf (дата звернення: 31.07.2024).
14. Конвенція про фізичний захист ядерного матеріалу і ядерних установок, 1980, поправки 2005. URL: https://www.iaea.org/publications/documents/infcircs/convention-on-the-physical-protection-of-nuclear-material (дата звернення: 31.07.2024).
15. Резолюція Ради Безпеки ООН 1373, 2001. URL: https://undocs.org/S/RES/1373(2001) (дата звернення: 31.07.2024).
16. Резолюція Ради Безпеки ООН 1540, 2004. URL: https://undocs.org/S/RES/1540(2004) (дата звернення: 31.07.2024).
17. Рамкова Конвенція Ради Європи про боротьбу з тероризмом, 2005. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196 (дата звернення: 31.07.2024).
18. Глобальна стратегія ООН з протидії тероризму, 2006. URL: https://www.un.org/counterterrorism/ctitf/un-global-counter-terrorism-strategy (дата звернення: 31.07.2024).
19. Директива Європейського Парламенту та Ради 2008/114/ЕС про ідентифікацію та позначення європейських критичних інфраструктур та оцінку потреб щодо їх захисту. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114 (дата звернення: 31.07.2024).
20. Міжнародна конвенція про боротьбу з фінансуванням тероризму (1999) URL: https://zakon.rada.gov.ua/laws/show/995_518 (дата звернення: 31.07.2024).
21. Конвенція ООН проти транснаціональної організованої злочинності (2000). URL: https://zakon.rada.gov.ua/laws/show/995_789 (дата звернення: 31.07.2024).
22. Закон України "Про критичну інфраструктуру" від16 листопада 2021 року № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 31.07.2024).