Anything else that Trump proposes will never be sustainable, as it will lack both legality and justice. Eventually, the world will have to return to the principles of international law – but the question is how many more lives will be lost before that happens. Ideally, as few as possible, because international law offers a way to prevent another disgrace like that of 1938 and the failed policy of appeasement before it escalates into a continental war costing tens of millions of lives.

Of course, Ukraine will have the final say – something that Trump's logic probably did not understand and calculate. Unilaterally imposing cynical deals will not be so easy for him. I hope that Europe will stand firmly with Ukraine on the side of law and justice.

Василь БЕРЕЗНЯК
завідувач кафедри кримінального права та кримінології, доктор юридичних наук, старший науковий співробітник

Діана РУКІНА
студентка ННІ права та інноваційної освіти

https://orcid.org/0000-0001-5690-4736

(Дніпровський державний університет внутрішніх справ, м. Дніпро, Україна)

МІЖНАРОДНО-ПРАВОВІ СТАНДАРТИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЇХ ІМПЛЕМЕНТАЦІЯ У КРИМІНАЛЬНЕ ПРАВО УКРАЇНИ

Захист об'єктів критичної інфраструктури є одним із ключових викликів сучасної міжнародної безпеки, оскільки вразливість таких об'єктів може мати катастрофічні наслідки для країн, населення та економіки. Як наслідок, у зв'язку із сучасними викликами створення універсальних міжнародно-правових стандартів, які забезпечували б ефективну координацію зусиль держав і міжнародних організацій у разі порушення функціонування об'єктів критичної інфраструктури, є невідкладним завданням. Водночас постає питання адаптації цих стандартів до національних правових систем, зокрема у сфері кримінального права, яке є важливим інструментом протидії злочинності.

У зв'язку з актуальністю досліджуваного питання значна кількість праць науковців у цій сфері зосереджувалась на формуванні міжнародних стандартів захисту критичної інфраструктури, зокрема у межах Організації Об'єднаних Націй (далі – ООН), Європейського Союзу (далі – ЄС) та Організація Північноатлантичного договору (далі – НАТО). Водночас увага приділяється порівняльно-правовому аналізу досвіду різних країн, що дозволяє виділити найефективніші підходи до адаптації міжнародних норм на національному рівні. Зокрема, серед найбільш ґрунтовних досліджень треба виокремити імена таких авторів: О. М. Герасименко, Гора І. В., Гуцалюк М. В., Захаров В. П., Колесник В. А., В. Д. Лювік, І. Р. Шинкаренко, О. О. Юріков та інші.

Для України, що перебуває у воєнному стані та зазнає кібернетичних і терористичних атак, проблема захисту критичної інфраструктури є дуже актуальною. Національне кримінальне законодавство потребує оновлення з урахуванням міжнародного досвіду для підвищення його ефективності. Часто імплементація міжнародно-правових норм стикається з проблемами, пов'язаними з їх адаптацією до національних реалій та забезпеченням належного механізму реалізації.

Законодавцем було внесено низку змін у кримінальному законодавстві з метою імплементації міжнародно-правових стандартів захисту критичної інфраструктури, враховуючи сучасні загрози та міжнародний досвід. Особлива увага приділяється боротьбі з кіберзлочинністю, тероризмом та диверсіями, які становлять найбільшу небезпеку для функціонування стратегічно важливих об'єктів.

Зокрема, ст. 361 Кримінального кодексу України (далі – КК України) передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних

машин, мереж та автоматизованих систем, що відповідає положенням Конвенції про кіберзлочинність [1; 2]. Посилення відповідальності за створення шкідливого програмного забезпечення закріплено в ст. 361-1 КК України, що спрямовано на попередження атак на критичну інфраструктуру [1]. У контексті протидії тероризму ст. 258 КК України визначає відповідальність за терористичні акти, включаючи дії, спрямовані на підрив критичної інфраструктури [1], що відповідає міжнародним стандартам, таким як Міжнародна конвенція про боротьбу з фінансуванням тероризму [3]. Водночас ст. 113 КК України, що регулює відповідальність за диверсію, охоплює діяння, які загрожують економічній чи оборонній спроможності держави, зокрема пошкодження об'єктів транспорту чи енергетики.

Значну увагу також приділено захисту енергетичної інфраструктури: ст. 194-1 КК України встановлює кримінальну відповідальність за умисне пошкодження об'єктів електроенергетики, що є вирішальними для національної безпеки [1]. Крім того, у статтях 363 та 363-1 КК України регулюються питання відповідальності за порушення правил експлуатації автоматизованих систем, які використовуються в критичних об'єктах, а ст. 360 КК України спрямована на захист засобів зв'язку, які є невід'ємною частиною критичної інфраструктури, де умисне руйнування або пошкодження телекомунікаційних мереж може призвести до масштабних збоїв у функціонуванні державних органів, транспортних систем, медичних закладів та інших важливих об'єктів. Особливо це актуально в умовах гібридних загроз, коли атаки на інфраструктуру зв'язку використовуються як частина загальної стратегії дестабілізації держави [1; 4, с. 45].

У контексті захисту критичної інфраструктури КК України також передбачає норми, спрямовані на протидію кримінальним правопорушенням, які можуть створювати загрозу для об'єктів стратегічного значення, зокрема ст. 259 КК України встановлює кримінальну відповідальність за умисне поширення неправдивої інформації про мінування чи інші загрози, що можуть викликати масові евакуації або інші надзвичайні заходи [5, с. 788]. Ця норма є важливою в контексті захисту критичної інфраструктури, оскільки фальшиві загрози щодо стратегічних об'єктів, таких як електростанції, аеропорти або лікарні, не лише відволікають ресурси, але й можуть спричиняти значні економічні втрати та посилювати суспільну паніку.

У контексті зростання кількості загроз для критичної інфраструктури в Україні видається доцільним розглянути можливість формування окремої статті в КК України, яка б встановлювала відповідальність за посягання на об'єкти критичної інфраструктури, зокрема її виклад може бути таким: «Ч. 1. Умисне вчинення дій, спрямованих на пошкодження, знищення, блокування роботи або інше втручання в діяльність об'єктів критичної інфраструктури, якщо це створило загрозу життю чи здоров'ю людей, заподіяло значну матеріальну шкоду або призвело до зупинення їх функціонування. Ч. 2. Ті самі дії, вчинені в умовах воєнного стану або в період збройного конфлікту». Це дозволить:

1. Адаптувати закон про кримінальну відповідальність до змін у законодавстві та міжнародних стандартах. Оскільки перелік об'єктів критичної інфраструктури може змінюватися, норма не вимагатиме постійного оновлення тексту статті КК України.
2. Чітко визначити відповідальність за різні види посягань. У межах такої статті можна передбачити окремі кваліфікуючі ознаки (наприклад, вчинене у період воєнного або надзвичайного стану тощо).
3. Посилити інтеграцію міжнародно-правових стандартів. Норма дозволить враховувати рекомендації ООН, ЄС, НАТО та інших організацій, які приділяють значну увагу захисту критичних об'єктів.

Отже, підсумовуючи вищевикладене, можна стверджувати, що захист об'єктів критичної інфраструктури є одним із пріоритетів у забезпеченні національної безпеки України, особливо в умовах сучасних гібридних загроз. У чинному КК України передбачено низку статей, які регулюють відповідальність за посягання на об'єкти критичної інфраструктури, але питання систематизації цих норм залишається актуальним. Створення окремої бланкетної статті дозволить не лише узгодити кримінально-правові положення із міжнародними стандартами, але й забезпечити ефективнішу протидію кримінально-протиправним посяганням, враховуючи специфіку національної правової системи. Така стаття сприятиме точному визначенню відповідальності за дії, спрямовані на дестабілізацію функціонування об'єктів критичної інфраструктури, а також адаптації до змін у загрозах та законодавчому регулюванні.

---

1. Про внесення змін до Кримінального кодексу України щодо посилення відповідальності за мародерство : Закон України від 07.03.2022 № 2117-IX. URL: https://zakon.rada.gov.ua/laws/show/2117-20#Text.

2. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р.: станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

3. Міжнародна конвенція про боротьбу з фінансуванням тероризму, 2000. URL: https://zakon.rada.gov.ua/ laws/show/995_518#Text.

4. Кваліфікація окремих кримінальних правопорушень проти критично важливих об'єктів інфраструктури (ст. ст. 259, 360 КК України) : метод. рекомендації / кол. авт. Дніпро : ДДУВС, 2024. 132 с.

5. Рукіна Д. О., Березняк В. С. Поняття «об'єкти критичної інфраструктури». The 4th International scientific and practical conference «Current trends in scientific research development» (November 14–16, 2024) BoScience Publisher, Boston, USA. 2024. S. 784–790.

Вікторія БІЛА
доктор юридичних наук, доцент
(Український науково-дослідний інститут спеціальної техніки та судових експертиз СБУ, м. Київ, Україна)
https://orcid.org/0000-0002-8201-219X

Віталій БОНДАРЧУК
професор кафедри фінансово-економічної безпеки Національної академії Служби безпеки України (м. Київ, Україна),
кандидат юридичних наук, доцент
https://orcid.org/0000-0002-5145-8631

AMLA: НОВИЙ ОРГАН ЄС З ПРОТИДІЇ ФІНАНСУВАННЮ ТЕРОРИЗМУ ТА ЛЕГАЛІЗАЦІЇ (ВІДМИВАННЮ) ДОХОДІВ, ОДЕРЖАНИХ ЗЛОЧИННИМ ШЛЯХОМ

Регламентом Європейського Парламенту і Ради (ЄС) 2024/1620 від 31 травня 2024 року було утворено новий орган із протидії фінансуванню тероризму та легалізації (відмиванню) доходів, одержаних злочинним шляхом з наднаціональною юрисдикцією – AMLA (Authority for Anti-Money Laundering and Countering the Financing of Terrorism) [1].

В обґрунтування такого рішення було покладено те, що країни-члени ЄС застосовують різні підходи до компетенції підрозділів фінансової розвідки (далі – ПФР) та процедур фінансового моніторингу, що не лише ускладнює координацію між національними ПФР, а й створює загрози для ефективності функціонування механізмів протидії транскордонним злочинам, що пов'язані з фінансуванням тероризму та легалізацією (відмиванням) доходів, одержаних злочинним шляхом (далі – AML/CFT). Недоліки в організації фінансового моніторингу однієї країни можуть створювати ризики для функціонування всієї системи протидії легалізації доходів фінансуванню тероризму (далі – ML/FT) ЄС [2]. Крім того, були висловлені серйозні занепокоєння, що використання нових фінансових інструментів (криптовалюти, онлайн-платформи) дозволить терористичним організаціям збільшити рівень «маскування» транзакцій, що не лише підвищить рівень загроз у сфері фінансування тероризму, а й значно збільшить транскордонний елемент цієї протиправної діяльності.

Саме тому виникла необхідність в утворенні єдиного органу, що об'єднує зусилля ПФР держав-членів ЄС. Варто вказати, що утворення AMLA є частиною пакету реформ, спрямованого на реалізацію Плану дій щодо комплексної політики Союзу щодо запобігання відмиванню грошей і фінансуванню тероризму [3], яким, серед іншого, передбачено уніфікацію низки норм щодо фінансового моніторингу.

Саме тому одним із основних завдань AMLA стане забезпечення єдності практики застосування правил фінансового моніторингу та забезпечення високих стандартів його здійснення. Крім того, до сфери відповідальності AMLA буде віднесено створення можливостей для спільного аналізу даних фінансового моніторингу різними національними