УДК 340.004.02

ПРАВОВА ВІДПОВІДАЛЬНІСТЬ ЗА АТАКИ НА КІБЕРФІЗИЧНІ СИСТЕМИ: ЮРИДИЧНИЙ АСПЕКТ

А. М. Назарова
здобувачка вищої освіти першого (бакалаврського) рівня 2 курсу спеціальності «Право», навчально-науковий інститут права
Науковий керівник – ст. викладач О. В. Кубай

Національний університет водного господарства та природокористування, м. Рівне, Україна

У статті розглядається зростаюча загроза атак на кіберфізичні системи та необхідність вдосконалення правового регулювання для забезпечення ефективного захисту в цифрову еру. Особливу увагу приділено ситуації в Україні, яка через сучасну гібридну війну потребує термінового вдосконалення правових аспектів кіберзахисту.
Ключові слова: кіберфізичні системи, кіберзахист, правове регулювання, кіберпростір.

The article describes the growing threat of attacks on cyber-physical systems and the need to improve legal regulation to ensure effective protection in the digital era. Special attention is paid to the situation in Ukraine, which, due to modern hybrid warfare, needs urgent improvement of the legal aspects of cyber protection.
Keywords: cyber-physical systems, cybersecurity, legal regulation, cyberspace.

У світі, де технології стають невід'ємною частиною нашого повсякденного життя, атаки на кіберфізичні системи набувають все більшого значення. Цей новий виклик для суспільства породжує питання про правову відповідальність за такі атаки та необхідність вдосконалення правового регулювання в цифровій ері.

Кіберфізичні системи, які об'єднують фізичний та цифровий світи, стають цільовим об'єктом для кіберзлочинців. Їхні атаки можуть призвести до серйозних наслідків, починаючи від витоку конфіденційної інформації і закінчуючи збоєм в роботі критичних інфраструктурних об'єктів, таких як електростанції чи мережі транспорту. Однак, не зважаючи на серйозний характер цих загроз, питання правової відповідальності за атаки на кіберфізичні системи залишається складним і багатогранним [1, С. 168].

Насамперед потрібно визначити та узгодити міжнародні стандарти для оцінки правової відповідальності в кіберпросторі. Сучасні атаки часто перетинають національні кордони, тому міжнародне співробітництво та визначення стандартів можуть визначити ефективні механізми протидії кіберзлочинності. Важливо також враховувати особливості кіберпростору, де анонімність та важкість відстеження атакуючих ускладнюють встановлення відповідальності [2, С. 330].

Другий аспект стосується розроблення ефективної системи санкцій та покарань для осіб чи організацій, які вчиняють атаки на кіберфізичні системи. Покарання повинно бути пропорційним завданому збитку та відображати серйозність кіберзлочинності. Застосування санкцій може включати штрафи, судове переслідування та навіть екстрадицію у випадках міжнародної кіберзлочинності.

Не менш важливим є розвиток системи захисту та попередження. Вдосконалення кіберзахисту для запобігання атакам та виявлення порушень є ключовим елементом стратегії

боротьби з кіберзлочинністю. Освіта громадськості та фахівців у галузі кібербезпеки також є важливим чинником у побудові стійкого цифрового суспільства [3, С. 115].

Атаки на кіберфізичні системи викликають необхідність стрімкої реакції на рівні міжнародного співтовариства. Створення ефективної системи правової відповідальності, визначення стандартів та застосування санкцій є ключовими етапами у побудові стійкого кіберпростору. Тільки колективні зусилля та визначення чітких меж відповідальності можуть забезпечити безпеку та стійкість кіберфізичних систем у цифровому віці. В еру сучасної війни, де величезну роль відіграє цифровий фронт, Україна, як і інші країни, знаходиться перед терміновою необхідністю врегулювання юридичного аспекту кіберзахисту. Злочинні атаки на кіберфізичні системи, особливо в контексті гібридної війни, визначають не лише новий вимір безпеки, але й вимагають ефективного правового реагування.

Першочергово Україна має узгоджувати своє законодавство щодо кіберзахисту з міжнародними стандартами. Оскільки кіберзлочинці оперують в глобальному просторі, необхідно розробити і впровадити норми, які дозволяють спільно працювати з іншими країнами у вирішенні кіберзахисту. Ратифікація та активна участь у міжнародних конвенціях є ключовим елементом цього процесу.

Другий аспект стосується визначення відповідальності за кіберзлочини в українському законодавстві. Важливо визначити поняття та класифікацію кіберзлочинці, а також передбачити адекватні санкції для осіб чи організацій, які вчиняють атаки на кіберфізичні системи. Застосування санкцій повинно бути прозорим і враховувати збитки, завдані національній безпеці та економіці [4, С. 113].

Окремий виклик для українського законодавства – це забезпечення відповідальності державних структур та органів, які мають відповідати за кіберзахист. Забезпечення прозорості та ефективності державних заходів у кіберпросторі є важливою умовою для успішної боротьби з кіберзлочинністю.

Зокрема, необхідно акцентувати увагу на впровадженні передових технічних та технологічних засобів для виявлення та захисту від кібератак. Розробка та впровадження системи реагування на інциденти є невід'ємною частиною такого підходу.

Отже, кіберзахист в Україні в контексті сучасної війни вимагає виваженого та комплексного юридичного підходу. Співпраця на міжнародному рівні, визначення відповідальності та створення ефективних механізмів захисту від кіберзлочинів – це лише деякі аспекти, які потрібно врахувати в українському законодавстві. Лише такий комплексний підхід може забезпечити стабільність та безпеку, коли кіберзахист стає необхідністю для національної безпеки та економічного розвитку.

1. Музика В. В. Проблема атрибуції кібератак проти об'єктів критичної інфраструктури та шляхи її вирішення в міжнародному праві. *Юридичний вісник*. 2020. № 4. С. 164–171. **2.** Музика В. В. Кібератаки та міжнародне право: природа та аналіз opinio juris держав щодо застосування міжнародного права в кіберпросторі. *Проблеми публічного та приватного права* : колект. моногр. / за заг. ред. Н. В. Мішиної. 2021. С. 309–342. **3.** Мельник Д. Національна критична інформаційна інфраструктура України: сучасні потреби захисту її об'єктів. *Збірник наукових праць НА СБУ*. Київ, 2019. № 70. С. 111–119. **4.** Мельник Д. Щодо актуальних потреб захисту національної критичної інформаційної інфраструктури України. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф. (Київ, 30.03.2018). Київ : Нац. акад. СБУ, 2018. С. 112–115.