DOI: https://doi.org/10.71404/PPSS.2024.2.48

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ: МІЖНАРОДНИЙ ДОСВІД ТА ВІТЧИЗНЯНА ПРАКТИКА

Богдан Олександрович МЕЛЬНИК,

аспірант відділу аспіранури (ад'юнктури) і докторантури Харківського національного університету внутрішніх справ

Інформаційна безпека є важливою складовою національної безпеки будь-якої держави, особливо в умовах воєнного стану. Сучасні конфлікти характеризуються активним використанням інформаційного простору для досягнення військових, політичних і економічних цілей. Це вимагає від держав розробки ефективного адміністративно-правового механізму, спрямованого на забезпечення інформаційної безпеки, враховуючи як національні особливості, так і міжнародний досвід.

Адміністративно-правовий механізм забезпечення інформаційної безпеки є комплексною системою, яка поєднує в собі правові, інституційні та процедурні інструменти для захисту інформаційного простору держави. Цей механізм базується на чітко визначених правових нормах, які регулюють порядок функціонування інформаційної сфери, а також окреслюють межі дозволеного та відповідальність за порушення правил. Законодавча база є фундаментом цього механізму, адже саме вона формує правову основу для діяльності державних інституцій у сфері забезпечення інформаційної безпеки. Важливу роль відіграють органи державної влади, які відповідають за контроль і регулювання в цій сфері. Їхня діяльність зосереджена на виявленні, попередженні та нейтралізації інформаційних загроз, що можуть мати негативний вплив на національну безпеку, стабільність та суверенітет держави[1]. Крім того, ці органи забезпечують виконання міжнародних зобов'язань у сфері інформаційної безпеки, що дозволяє інтегрувати національну систему захисту у глобальний контекст. Процедури реагування на інформаційні загрози є ще одним ключовим елементом цього механізму. Вони включають заходи з кіберзахисту, зокрема моніторинг, виявлення і протидію кіберзагрозам, а також боротьбу з дезінформацією та іншими формами інформаційного впливу. Ефективність таких процедур залежить від використання сучасних технологій, оперативності ухвалення рішень та професійності фахівців, які реалізують ці заходи.

Злагоджена робота всіх елементів механізму є вирішальною для його успішного функціонування. Координація між різними державними органами, постійне вдосконалення нормативно-правової бази, розвиток

технічних можливостей та залучення експертного потенціалу сприяють створенню ефективної системи захисту національного інформаційного простору[2]. Це особливо важливо в умовах сучасних викликів, коли інформаційна безпека стає ключовим елементом загальної системи національної безпеки.

Міжнародний досвід забезпечення інформаційної безпеки демонструє широкий спектр підходів і механізмів, які використовуються різними державами для захисту свого інформаційного простору. У США ефективність системи кібербезпеки забезпечується завдяки комплексному підходу, основою якого є співпраця між державними органами, приватним сектором і науковими установами. Центральну роль відіграє Агентство кібербезпеки та інфраструктурної безпеки (CISA), яке координує заходи із захисту критичної інфраструктури, реагування на кібератаки та проведення роз'яснювальної роботи серед громадян і підприємств. Особливість американської моделі полягає в її гнучкості та здатності адаптуватися до швидких змін у технічній сфері, а також у залученні приватних компаній до розробки рішень у сфері кіберзахисту[3]. У Європейському Союзі забезпечення інформаційної безпеки здійснюється в рамках єдиної нормативно-правової системи, яка дозволяє країнам-членам співпрацювати для захисту спільного цифрового простору. Важливу роль відіграє Директива NIS2, що встановлює мінімальні вимоги до кібербезпеки для всіх держав ЄС. Водночас Агентство ЄС з кібербезпеки (ENISA) забезпечує координацію та підтримку зусиль країн-членів, пропонуючи експертні рекомендації, організовуючи навчання та тренування з реагування на інциденти[4]. Особливістю європейського підходу є акцент на регіональній співпраці та взаємодії між державами для забезпечення цілісності інформаційного простору ЄС. Ізраїль відомий своєю передовою системою забезпечення інформаційної безпеки, яка інтегрує інноваційні технології, державну політику та активну участь приватного сектору. У цій країні працює потужна система реагування на кіберзагрози, яка базується на високому рівні підготовки фахівців і розвиненій інфраструктурі для моніторингу та протидії кіберзлочинам. Ізраїль активно підтримує розвиток стартапів у сфері кібербезпеки, що дозволяє постійно вдосконалювати технології та методи захисту. Особливістю цієї моделі є інтеграція військових технологій у цивільний сектор, що значно підвищує її ефективність.

Загалом успішний досвід інших країн свідчить, що ефективна система забезпечення інформаційної безпеки базується на комплексному підході, який включає сучасні технічні рішення, ефективне законодавче регулювання, співпрацю між державним і приватним секторами, а також інтеграцію в міжнародну систему протидії кіберзагрозам. Це створює умови для захисту інформаційного простору від сучасних викликів та загроз.

Національна практика України у сфері інформаційної безпеки набула особливої важливості в умовах воєнного стану, що вимагає швидкої адаптації до нових викликів і загроз у цій сфері. Законодавчі

ініціативи стали ключовим інструментом для створення належної правової основи, яка регулює порядок забезпечення інформаційної безпеки. Зокрема, Закон України "Про основні засади забезпечення кібербезпеки України" визначає принципи, механізми і завдання у сфері кіберзахисту, створюючи основу для координації діяльності державних органів та інших учасників[5]. Також були прийняті закони, спрямовані на боротьбу з дезінформацією, блокування пропагандистських ресурсів та посилення інформаційного суверенітету. Інституційні зміни стали важливим кроком для формування ефективного механізму забезпечення інформаційної безпеки. Зокрема, Державна служба спеціального зв'язку та захисту інформації України виконує роль центрального органу виконавчої влади, відповідального за координацію заходів у цій сфері. Її діяльність охоплює як оперативне реагування на кіберзагрози, так і стратегічне планування у сфері інформаційного захисту. Крім того, було посилено функції інших державних органів, таких як Міністерство цифрової трансформації, яке активно займається впровадженням технологічних рішень для підвищення кіберзахисту. Міжнародна співпраця є важливим компонентом української практики у сфері інформаційної безпеки. Уряд активно співпрацює з міжнародними організаціями, зокрема НАТО, Європейським Союзом, ОБСЄ та іншими партнерами. Ця співпраця включає технічну підтримку, обмін досвідом, спільні тренування та участь у розробці міжнародних стандартів кібербезпеки. Завдяки цим зусиллям Україна отримує доступ до передових технологій, знань і ресурсів, що значно підвищує її спроможність протистояти сучасним інформаційним загрозам.

На нашу думку, попри значний прогрес, Україна стикається з низкою викликів, які потребують негайного вирішення. Серед них – необхідність посилення кадрового потенціалу у сфері кібербезпеки, що включає підготовку висококваліфікованих спеціалістів та запровадження сучасних навчальних програм. Крім того, модернізація технічної бази залишається пріоритетом, оскільки наявна інфраструктура часто не відповідає вимогам сучасного інформаційного середовища. Важливо також продовжувати вдосконалення нормативно-правової бази, забезпечуючи її відповідність не лише національним потребам, а й міжнародним стандартам. Лише за умови подолання цих викликів Україна зможе ефективно забезпечувати інформаційну безпеку в умовах сучасних викликів.

Отже, адміністративно-правовий механізм забезпечення інформаційної безпеки є важливим інструментом для захисту національних інтересів в умовах сучасних викликів. Міжнародний досвід свідчить, що ефективна система захисту вимагає комплексного підходу, інтеграції зусиль державного та приватного секторів, а також міжнародної співпраці. Для України, яка перебуває в умовах воєнного стану, першочерговими завданнями є адаптація національної практики до сучасних викликів та врахування найкращих світових практик. Це

дозволить створити надійний фундамент для забезпечення інформаційної безпеки й захисту державного суверенітету.

Список використаних джерел

1.Авраменко С.В. Забезпечення інформаційної безпеки в умовах збройних конфліктів: адміністративно-правові аспекти. *Право України. 2022. № 10. С. 34-41. DOI: https://doi.org/10.33445/pu.2022.10.4.*

2.Бондаренко Т.П. Інформаційна безпека в умовах воєнного стану: законодавчий аспект. *Матеріали міжнародної науково-практичної конференції «Інформаційні технології в правовій системі». Київ. КНУ ім. Т. Шевченка. 2023. С. 45-52.*

3.Голубенко О.В. Адміністративно-правовий механізм забезпечення кібербезпеки: міжнародний досвід. *Журнал східноєвропейського права. 2023. № 5. С. 28-33.*

4.Коваленко Р.М. Національна стратегія інформаційної безпеки України: виклики та перспективи. *Безпека інформаційного простору України. Харків. Юридичний науковий журнал. 2024. С. 89-96.*

5.Петренко І.О., Малишева Л.В. Інтеграція міжнародного досвіду в національну систему кібербезпеки України. *Науковий вісник Національного юридичного університету ім. Ярослава Мудрого. 2024. № 3. С. 73-78. DOI: https://doi.org/10.31733/nyu.2024.3.10.*