ОСОБЛИВОСТІ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ: НАЦІОНАЛЬНИЙ І МІЖНАРОДНИЙ ДОСВІД

Богдан Олександрович МЕЛЬНИК,

аспірант відділу організації освітньо-наукової підготовки Харківського національного університету внутрішніх справ

В умовах глобальної діджиталізації питання інформаційної безпеки набувають особливої актуальності. Збройні конфлікти сучасності демонструють значний вплив інформаційних загроз на політичну, економічну та соціальну стабільність держав. Під час дії правового режиму воєнного стану регулювання інформаційної безпеки стає ключовим елементом державної безпеки.

В Україні адміністративно-правове регулювання інформаційної безпеки в умовах воєнного стану має комплексний характер і ґрунтується на низці ключових нормативно-правових актів. До основних документів, які забезпечують правове підґрунтя у цій сфері, належать Конституція України, Закон України "Про основи національної безпеки України", Закон України "Про інформацію" та Закон України "Про правовий режим воєнного стану". Ці акти визначають загальні принципи забезпечення інформаційної безпеки, окреслюють обов'язки державних органів, права громадян та юридичних осіб, а також встановлюють порядок взаємодії суб'єктів у сфері захисту інформаційного простору.

Введення воєнного стану дозволяє державі застосовувати додаткові заходи для протидії інформаційним загрозам. До таких заходів належить тимчасова заборона роботи засобів масової інформації, які поширюють дезінформацію або ворожу пропаганду, що здатна завдати шкоди національній безпеці. Держава отримує право блокувати доступ до інтернет-ресурсів, які використовуються для поширення шкідливих даних або здійснення психологічного впливу на населення. Одним із ключових аспектів є посилення контролю за обігом інформації, яка має стратегічне значення, зокрема щодо критичної інфраструктури, оборонної промисловості та діяльності органів державної влади. У контексті адміністративних механізмів захисту інформаційної безпеки важливу роль відіграють спеціалізовані органи, які здійснюють моніторинг, аналіз і реагування на інформаційні загрози. До таких органів належать Служба безпеки України, Національна рада з питань телебачення і радіомовлення та кіберполіція. Служба безпеки України виконує функцію стратегічного координатора у сфері інформаційної безпеки, забезпечуючи оперативне виявлення та нейтралізацію загроз. Водночас Національна рада здійснює контроль за дотриманням вимог щодо змісту інформації, що поширюється через засоби масової інформації. Кіберполіція, у свою чергу, займається протидією кіберзлочинам, які пов'язані з розповсюдженням шкідливого контенту або кібератаками на інформаційні ресурси держави. Практичне застосування цих адміністративних механізмів демонструє їхню ефективність у боротьбі з інформаційними загрозами. Зокрема, успішна протидія російській пропаганді та нейтралізація масштабних кампаній дезінформації стали можливими завдяки тісній співпраці державних органів і громадянського суспільства. Важ-

ливу роль у цьому відіграє швидке реагування на появу фейкових новин, які спрямовані на деморалізацію населення або дискредитацію військово-політичного керівництва країни.

На нашу думку, важливою складовою є проведення інформаційно-просвітницьких кампаній, спрямованих на підвищення обізнаності громадян щодо методів протидії дезінформації. Це дозволяє мінімізувати вплив ворожих інформаційних атак, одночасно підвищуючи стійкість українського суспільства до зовнішніх маніпуляцій. Таким чином, адміністративно-правові заходи забезпечення інформаційної безпеки під час воєнного стану формують цілісну систему захисту, яка відповідає сучасним викликам та сприяє зміцненню національної безпеки.

Міжнародний досвід регулювання інформаційної безпеки в умовах надзвичайного стану демонструє значну різноманітність підходів, які залежать від правової системи, технічного розвитку та характеру загроз, що стоять перед конкретними державами. Європейський Союз приділяє значну увагу забезпеченню інформаційної безпеки, розглядаючи її як важливу складову своєї загальної безпекової стратегії. Важливим нормативним документом, який регулює сферу кібербезпеки в ЄС, є Директива NIS2. Вона встановлює єдині мінімальні вимоги до захисту інформаційних систем у державах-членах, а також передбачає створення механізмів обміну інформацією між країнами для оперативного реагування на кіберзагрози. У контексті надзвичайного стану країни ЄС використовують комплексний підхід, який включає співпрацю з приватним сектором, зокрема провайдерами послуг і технологічними компаніями, для виявлення потенційних загроз. Координація між державами-членами дозволяє оперативно реагувати на дезінформаційні кампанії та протидіяти маніпулятивному впливу, який часто має міжнаціональний характер. Крім того, значна увага приділяється підвищенню цифрової грамотності населення. Інформаційно-просвітницькі програми допомагають громадянам розпізнавати неправдиві повідомлення та уникати маніпуляцій. Особливої уваги заслуговує досвід країн Балтії – Латвії, Литви та Естонії. Ці держави вже тривалий час стикаються з інтенсивними інформаційними атаками з боку Росії. Вони запровадили ефективні моделі правового та технологічного захисту, які включають не лише блокування ворожих інформаційних джерел, але й активне використання контрнаративів для нейтралізації пропаганди. У цих країнах широко застосовуються сучасні технології моніторингу інформаційного простору, а також законодавчі ініціативи, які дозволяють швидко реагувати на загрози. Сполучені Штати Америки демонструють інший підхід до регулювання інформаційної безпеки, базуючись на поєднанні жорстких законодавчих заходів і гнучкої взаємодії з громадянським суспільством. Закон про кібербезпеку та пов'язані з ним акти визначають основні принципи захисту інформаційного простору. У разі надзвичайного стану уряд США використовує централізовану систему управління інформаційною безпекою, ключовим елементом якої є Агентство кібербезпеки та інфраструктурної безпеки (CISA). Це агентство координує дії федеральних, регіональних та приватних структур для забезпечення ефективного захисту від інформаційних загроз. Особливістю американської системи є широкий спектр правових механізмів, які дозволяють тимчасово блокувати джерела дезінформації або застосовувати санкції проти осіб і організацій, що поширюють небезпечний контент. Важливою складовою є робота з медіа, які залучаються до створення контрна-

ративів для протидії пропаганді. Це дає можливість не лише нейтралізувати вплив маніпулятивної інформації, але й зміцнювати довіру громадян до офіційних джерел. У США також активно впроваджуються освітні програми, спрямовані на підвищення обізнаності населення щодо методів боротьби з дезінформацією. Такий підхід сприяє формуванню стійкого суспільства, здатного протидіяти сучасним викликам у сфері інформаційної безпеки. Міжнародний досвід доводить, що ефективне регулювання інформаційної безпеки в умовах надзвичайного стану потребує комплексного підходу, який об'єднує правові, технологічні та освітні заходи.

Підсумовуючи вище викладене можна стверджувати, що адміністративно-правове регулювання інформаційної безпеки в умовах правового режиму воєнного стану має важливе значення для забезпечення національної безпеки. Український досвід демонструє ефективність застосування законодавчих механізмів і міжвідомчої координації. Водночас міжнародні практики, зокрема досвід ЄС і США, свідчать про важливість інтеграції сучасних технологій, підвищення цифрової грамотності населення та міжнародної співпраці у цій сфері. Для України подальший розвиток системи інформаційної безпеки має включати адаптацію найкращих міжнародних практик, удосконалення нормативної бази та посилення співпраці з партнерами.