Миронова Д. С.,
здобувачка вищої освіти Навчально-наукового інституту права та соціального менеджменту, Донецький державний університет внутрішніх справ
(м. Кропивницький, Україна)

Науковий керівник:
Куракін О. М.,
доктор юридичних наук, професор, професор кафедри державно-правових дисциплін Навчально-наукового інституту права та соціального менеджменту, Донецький державний університет внутрішніх справ,
(м. Кропивницький, Україна)

ІМПЛЕМЕНТАЦІЯ МІЖНАРОДНОГО ДОСВІДУ У СФЕРІ БОРОТЬБИ З ГІБРИДНИМИ ЗАГРОЗАМИ В УКРАЇНІ

Сучасна безпекова ситуація в Україні характеризується активним впливом гібридних загроз, які поєднують інформаційні, кібернетичні, психологічні та економічні інструменти впливу. Вони здатні підривати стабільність державних інститутів, дестабілізувати суспільство та впливати на прийняття стратегічних рішень. У цьому контексті імплементація міжнародного досвіду є критично важливою для розвитку адаптивної та ефективної системи національної безпеки України [1, 2]. Особливо це актуально для України з огляду на тривалий збройний конфлікт та системну інформаційну агресію з боку РФ, що робить потребу в міжнародних моделях реагування життєво необхідною.

Міжнародна інтеграція, насамперед у форматі співпраці з ЄС і НАТО, відкриває доступ до передових правових стандартів та методик протидії гібридним загрозам, зокрема у сфері стратегічних комунікацій, захисту інформаційного простору та забезпечення безпеки критичної інфраструктури.

Аналіз законодавчих підходів та організаційних механізмів, що застосовуються в Європейському Союзі для протидії гібридній агресії, а також практичних інструментів стратегічної взаємодії з НАТО [4], дозволяє виділити ключові принципи ефективного реагування на комплексні безпекові ризики. У в інформаційній довідці висвітлюються особливості нормативного регулювання, інституційної координації та багаторівневої співпраці між державами-членами, що спрямовані на підвищення стійкості до комплексних безпекових впливів. Дослідження цих практик є важливим для адаптації

європейського досвіду до українських реалій та формування ефективних нормативно-правових рамок діяльності державних органів у сфері інформаційної та національної безпеки. В Україні вже реалізуються активні заходи у цьому напрямі, зокрема через імплементацію Стратегії національної безпеки, Доктрини інформаційної безпеки та розвиток системи стратегічних комунікацій відповідно до стандартів НАТО.

Особливу увагу у контексті міжнародного досвіду заслуговує практика Словаччини, де ухвалено національні концепції протидії гібридним загрозам, що передбачають координацію між державними органами, правове регулювання та застосування стратегічних комунікацій. Аналіз міжнародної практики, зокрема документів ЄС та словацьких підходів, дозволяє виділити ключові принципи ефективного протидії гібридним загрозам та демонструє важливість інтеграції міждержавних механізмів для забезпечення інформаційної стійкості і безпеки критичної інфраструктури. На основі цього досвіду Україна може впроваджувати адаптовані моделі протидії гібридним загрозам, враховуючи національні специфіки та міжнародні стандарти [5].

Головним акцентом сучасних досліджень є формування зумовлена необхідністю формування комплексної системи захисту національних інтересів у сфері інформаційної безпеки, що включає правові, організаційні та технологічні механізми. Це передбачає вивчення міжнародних стандартів, нормативно-правових актів, а також передових практик ЄС та НАТО для створення ефективної, адаптивної та стійкої системи стратегічних комунікацій в Україні [2], [4]. Насамперед такі процеси вже розпочато, зокрема через створення Центру протидії дезінформації, реформування сектору кібербезпеки та інтеграцію українських стратегічних комунікацій у європейський безпековий простір.

Гібридні загрози, що виникають у сучасних умовах інформаційної війни, вимагають системного правового та організаційного підходу. Одним із ключових елементів такого підходу є розробка і впровадження нормативно-правових актів, що регулюють діяльність державних органів у сфері протидії дезінформації та кібератакам. В Україні нормативно-правова база поступово адаптується до міжнародних стандартів, у тому числі у сфері стратегічних комунікацій та інформаційної безпеки, що передбачає визначення правових основ функціонування інформаційно-аналітичних центрів, методологій оцінки впливу дезінформації на суспільну стабільність, а також застосування технологій моніторингу та аналітики інформаційного простору [1, 4].

Згідно з аналітичними матеріалами [4], правове забезпечення міжнародного співробітництва України у сфері протидії гібридним загрозам передбачає застосування міжнародних угод, норм ЄС та стандартів НАТО, що дозволяє підвищити ефективність державної політики у сфері інформаційної безпеки. Особливу увагу приділено законодавчому визначенню механізмів стратегічних комунікацій, оцінки загроз та взаємодії з міжнародними партнерами.

Важливою складовою є також впровадження стратегічних комунікацій як інструменту захисту інформаційного простору та формування суспільної стійкості. Україна активно переймає практики ЄС, зокрема принципи координації між державними органами та об'єднання зусиль з міжнародними партнерами, що дозволяє підвищити ефективність реагування на дезінформаційні кампанії та гібридні атаки [3, 5]. Водночас українські інституції активно беруть участь у спільних навчаннях, інформаційних кампаніях та аналітичних програмах ЄС, спрямованих на розвиток стійкості демократичних інститутів.

Крім того, міжнародна інтеграція сприяє розвитку правових та технологічних механізмів, що дозволяють не лише реагувати на сучасні загрози, а й прогнозувати потенційні виклики. Поєднання нормативно-правових рішень, технологічних інструментів та системи стратегічних комунікацій дозволяє створити адаптивну систему безпеки, яка здатна забезпечити комплексний захист національних інтересів та інформаційної інфраструктури [2, 4, 5].

Системна імплементація міжнародного досвіду формує стійку та ефективну систему національної безпеки, яка відповідає сучасним викликам та міжнародним стандартам. При цьому акцент робиться на комплексному підході, що включає нормативно-правове регулювання, технологічні засоби моніторингу та аналітики, а також активне використання стратегічних комунікацій для зміцнення інформаційної стійкості суспільства [4, 5].

У процесі здійсненого аналітичного опрацювання було комплексно розглянуто сучасні підходи до протидії гібридним загрозам в Україні з урахуванням міжнародного досвіду ЄС, НАТО та окремих держав, зокрема Словаччини. Ми виявили, що ефективна система національної безпеки потребує комплексного поєднання правових, організаційних і технологічних механізмів, що дозволяють не лише реагувати на існуючі загрози, а й прогнозувати потенційні виклики.

Аналіз законодавства, міжнародних стандартів та практик стратегічних комунікацій показав, що імплементація міжнародного досвіду дозволяє Україні створити адекватну правову базу та організаційні моделі для забезпечення інформаційної стійкості суспільства та захисту національних інтересів [1, 2]. Досвід країн демонструє практичну ефективність координації між державними органами, інтеграції стратегічних комунікацій та партнерської взаємодії з міжнародними структурами, що є важливим для адаптації українських механізмів реагування [5].

Важливою перспективою подальших досліджень є розробка комплексних моделей оцінки ризиків та прогнозування інформаційних загроз з урахуванням специфіки українського контексту.

Отже, системна імплементація міжнародного досвіду формує стійку, адаптивну та ефективну систему національної безпеки України, яка здатна протидіяти сучасним гібридним загрозам, захищати критичну інформаційну інфраструктуру та забезпечувати довгострокову стабільність держави. Реалізація таких підходів сприятиме зміцненню національної безпеки та

відповідності України міжнародним стандартам у сфері протидії гібридним загрозам.

У цьому контексті Україна виступає не лише країною, яка адаптує міжнародний досвід, а й важливим генератором власних практик, що формуються в умовах реальної гібридної війни та можуть бути інтегровані у глобальну систему безпеки.

Список використаних джерел:

1. Ільницька У. Безпековий вимір зовнішньополітичних інформаційно-комунікативних стратегій Європейського Союзу. Політична наука: зб. наук. праць. 2025. Вип. 1. С. 68-75.
2. Karpenko, O. Hybrid Threats: Legal and Security Aspects in the Ukrainian Context. International Economic Policy Journal. 2024. №41. С. 177-185.
3. Підходи Словаччини до боротьби з гібридними загрозами: аналітика від експерта НІСД. Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/news/statti/pidkhodi-slovachchini-do-borotbi-z-gibridnimi-zagrozami-analitika-vid-eksperta-nisd
4. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України: «Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій».URL: https://infocenter.rada.gov.ua/uploads/documents/29377.pdf
5. Королюк Т. О., Чворун К. Г. Стратегічні комунікації як засіб у боротьбі з дезінформації. Вісник Київського нац. економ. ун-ту. 2023. №53. С. 52-58. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/1998262