УДК 327.56

Бошян А.А., студент групи НБМ-4
Державний університет «Житомирська політехніка»

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ БОРОТЬБИ ФІНАНСУВАННЯ ТЕРОРИЗМУ

Актуальність теми: У сучасних умовах загрози національній безпеці на території України фінансування тероризму займає одне з ключових місць. Це явище стало не лише кримінальною проблемою, а й інструментом політичного тиску та дестабілізації державності. Боротьба з фінансуванням тероризму вимагає постійного вдосконалення механізмів виявлення, запобігання та протидії. Актуальність теми зумовлена необхідністю формування ефективної системи фінансового моніторингу та правозастосовної практики, що відповідала б сучасним викликам та загрозам у сфері національної безпеки.

Мета дослідження: обґрунтування та вдосконалення теоретико-методологічних підходів до боротьби з фінансуванням тероризму як складової системи забезпечення національної безпеки України.

Тероризм є одним із найнебезпечніших соціальних явищ сучасності, що становить глобальну загрозу як для окремих держав, так і для міжнародної спільноти в цілому. Відповідно до статті 1 Закону України «Про боротьбу з тероризмом», тероризм – це злочинна діяльність, що полягає у застосуванні насильства або загрози його застосування з метою порушення громадської безпеки, залякування населення, провокації збройного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень органами державної влади або місцевого самоврядування, посадовими особами, об'єднаннями громадян, юридичними особами. Це визначення охоплює як внутрішні, так і міжнародні прояви тероризму, а також наголошує на цілеспрямованості дій терористів [1]. З позиції кримінального права, тероризм розглядається як злочин особливої тяжкості, який має транснаціональний характер і вимагає комплексної протидії з боку держави.

Одним із видів широкого спектру дій терористичної діяльності є її фінансування [2, с. 144]. Фінансування тероризму є матеріальною основою, яка спричиняє загибель багатьох людей внаслідок терористичних актів, диверсійно-підривної діяльності або військової агресії. У цьому контексті терористи та інші злочинці активно застосовують сучасні механізми відмивання грошей для приховування справжніх джерел своїх фінансових активів та злочинних доходів. Саме фінансові ресурси дозволяють таким структурам не лише здійснювати терористичні атаки, а й підтримувати свою діяльність на постійній основі, забезпечувати функціонування інфраструктури, утримувати членів організації, поширювати ідеологію та розширювати вплив. Потреба в коштах особливо гостро постає перед великими терористичними структурами, які прагнуть контролювати території або вести тривалу протидію державній владі. Для підтримки ефективності діяльності терористи створюють складні фінансові мережі, які дають змогу систематично отримувати прибутки. Їхні фінансові пріоритети залежать від поточних завдань, етапу розвитку організації, її масштабів та цілей. Фінансування тероризму доцільно розглядати у двох вимірах – юридичному та фінансовому. Правовий вимір передбачає поділ джерел фінансування на легальні й нелегальні, відстеження та аналіз усіх фінансових операцій, які здійснюються терористами, а також розробку відповідних норм законодавства для протидії цим діянням і притягнення винних до відповідальності. Фінансовий вимір акцентує увагу на джерелах надходження коштів – від самофінансування до зовнішньої підтримки, і передбачає розробку заходів, спрямованих на скорочення обсягів ресурсів, доступних для терористичних організацій [3, с. 64].

Основні напрями використання фінансів терористичними організаціями включають [4, с. 110-111]:

1. Проведення терористичних операцій. Це вимагає значних витрат для підготовки та реалізації терактів. Необхідно фінансувати попередню розвідку об'єкта атаки, переміщення учасників, придбання зброї (як вогнепальної, так і вибухових пристроїв), виготовлення підроблених документів, забезпечення логістики, транспортних засобів, тимчасового житла, харчування, медичної допомоги тощо.
2. Пропагандистська діяльність і вербування для залучення нових членів, формування лояльного середовища та легітимізацію ідеології. Розвинені терористичні організації створюють цілі медіа-комплекси – сайти, онлайн-журнали, газети, домени, а подекуди навіть контролюють телерадіоканали для пропагування своїх поглядів і мобілізації ресурсів.
3. Підготовка на навчання кадрів. Терористичні угрупування інвестують кошти у навчання своїх бійців, щоб забезпечити високий рівень ефективності дій.
4. Матеріальна підтримка членів та їх родин. Фінансова винагорода відіграє важливу роль у формуванні лояльності та мотивації своїх учасників. Це створює видимість турботи та стимулює залучення нових осіб до діяльності.
5. Створення та підтримка соціальних послуг. Деякі терористичні організації використовують частину фінансових надходжень на розбудову соціальної інфраструктури з метою сформувати довіру серед місцевого населення.

На практиці, при реалізації заходів щодо виявлення ознак зазначеного правопорушення, виникає потреба у глибшому теоретичному обґрунтуванні. У контексті кримінологічної характеристики фінансування тероризму Д.С. Мельник і Б.Д. Леонов виділяють три основні складові:

1. Кількісні та якісні показники, до яких належать: загальна кількість зафіксованих злочинів відповідного характеру, їх поширеність, частка у структурі злочинності, динаміка змін, структура та вартість фінансування тероризму, а також його географічне розповсюдження;

2. Причини, умови вчинення таких злочинів і взаємозв'язки між ними;

3. Дані щодо характерних рис особистостей, які здійснюють фінансову підтримку терористичних структур (спонсорів тероризму) [5, с. 90–91].

Серед зазначених факторів особливу увагу варто приділити саме тим, що мають суто фінансовий характер – тобто, чинникам, які обумовлюють фінансування тероризму, а також взаємозв'язкам між ними.

Дослідження механізмів фінансування тероризму повинне враховувати комплексний вплив різних чинників, зокрема: обсяг ресурсів, необхідних для реалізації стратегії терористичної організації; обмеження, продиктовані її ідеологією у взаємодії зі злочинним світом; внутрішня структура угруповання, а також його здатність управляти фінансовими потоками й кримінальними зв'язками. Останніми роками в Україні сформувалась нормативно-правова база, яка узгоджується з міжнародними стандартами і створює підґрунтя для виявлення й блокування фінансових операцій, пов'язаних з терористичною діяльністю[6, с. 82]. Ефективна боротьба з тероризмом неможлива без чіткого нормативного регулювання. У цій сфері діє значна кількість як національних, так і міжнародних правових документів. До основних належать: Конституція України, Кримінальний кодекс України, закони «Про боротьбу з тероризмом», «Про основи національної безпеки України», «Про Службу безпеки України», «Про Національну поліцію», «Про контррозвідувальну діяльність», «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом», а також «Положення про Антитерористичний центр». Серед міжнародних документів слід виокремити Європейську конвенцію про боротьбу з тероризмом, Конвенцію Ради Європи про запобігання тероризму, а також низку галузевих угод, що регулюють окремі аспекти, зокрема бомбовий, ядерний та фінансовий тероризм [7, с. 76]. Найбільш важливим з точки зору протидії фінансуванню тероризму є Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом». У цьому законі міститься пряме посилання на необхідність виявлення, оцінювання і зменшення ризиків фінансування тероризму. Документ зобов'язує фінансові установи, банки, страхові компанії, нотаріусів, аудитора та інших суб'єктів фінансового моніторингу здійснювати належну перевірку клієнтів, повідомляти про підозрілі фінансові операції, що можуть бути пов'язані з фінансуванням терористичної діяльності. Запроваджено механізм ризик-орієнтованого підходу, який дозволяє державі фокусуватися на найбільш загрозливих напрямках. Дані нормативно-правові засади в Україні засвідчують наявність цілісної законодавчої бази, яка охоплює як кримінальну відповідальність за фінансування тероризму, так і превентивні заходи фінансового моніторингу.

Висновок: Фінансування тероризму є невід'ємним компонентом терористичної діяльності, що забезпечує ресурсну базу для її здійснення. Воно включає як легальні, так і нелегальні джерела надходження коштів, включаючи відмивання грошей, тіньову економіку, корупційні схеми тощо. Це робить боротьбу з фінансуванням тероризму одним із ключових напрямів забезпечення національної та міжнародної безпеки. В Україні створена багаторівнева, скоординована система протидії тероризму, яка базується на чіткій регламентації повноважень, взаємодії між органами влади, своєчасному реагуванні та превентивній діяльності. Вона є динамічною і постійно адаптується до нових викликів, зокрема в умовах гібридної агресії та міжнародного тероризму.

Список використаних джерел:

1. Про боротьбу з тероризмом: Закон України від 20 березня 2003 року № 638-IV. Відомості Верховної Ради України (ВВР), 2003, № 25, ст.180. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text.

2. Токарчук О. В. Запобігання терористичним актам. збірник матеріалів Наукового форуму. Навчально-науковий інститут права та політології УДУ імені Михайла Драгоманова (м. Київ, 21 червня 2023 р.). Київ: Вид-во УДУ імені Михайла Драгоманова, 2023. С. 144-146. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/41165/Protydiia%20terorystychnym%20aktam%20u%20miskomu%20seredovyshchi.pdf?sequence=1&isAllowed=y.

3. Грабчук І. Л., Власюк Т. О. Характеристика наслідків фінансування міжнародного тероризму як ключових векторів розвитку фінансового моніторингу. Економіка, управління та адміністрування. Вип. 1(107). 2024. С. 61–65. https://doi.org/10.26642/ema-2024-1(107)-61-65.

4. Баранов О. П. Фінансування тероризму як загроза національній безпеці. Державне управління. Інвестиції: практика та досвід. Вип. 9. 2018. С. 108-112. URL: http://www.investplan.com.ua/pdf/9_2018/22.pdf.

5. Мельник Д. С., Леонов Б.Д. Поняття та зміст кримінологічної характеристики фінансування тероризму. Інформація і право. 2022. Вип. 2. С. 85–93. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Infpr_2022_2_.

6. Рисін В.В., Степанова А.В. Інструменти протидії фінансуванню тероризму з використанням фінансових установ. економічна наука. Економіка та держава. Економічна наука. 2020. № 6. С. 80–86. URL: http://www.economy.in.ua/?op=1&z=4655&i=11.

7. Гбур З., Кошова С. Нормативно-правові засади боротьби з тероризмом в Україні. Аспекти публічного управління. Том 9. Вип. 1. 2021. С. 72-80.

УДК 336.71:343.35

Бошян А.А., здобувач освітнього ступеня магістр
Науковий керівник: Абрамова І.В., д.е.н., доц.,
доцент кафедри міжнародних відносин і політичного менеджменту
Державний університет «Житомирська політехніка»

АНАЛІЗ ТА ОЦІНКА РИЗИКІВ ВІДМИВАННЯ КОШТІВ У БАНКІВСЬКОМУ СЕКТОРІ

У сучасному глобалізованому світі, де грошові потоки швидко переміщуються між країнами, ризики відмивання коштів (відмивання доходів, отриманих злочинним шляхом) зростають. Банківський сектор відіграє ключову роль у фінансовій системі кожної країни і, разом з тим, є вразливим до використання у схемах легалізації злочинних коштів. Злочинці постійно вдосконалюють свої методи, використовуючи новітні технології та складні схеми для маскування незаконного походження коштів. Банківський сектор охоплює широкий спектр послуг, включаючи відкриття та обслуговування рахунків, переказ коштів, кредитування, обмін валют, зберігання цінностей, інвестиційне обслуговування тощо. Його важливість полягає в тому, що всі ключові фінансові потоки проходять через банки, що робить цей сектор особливо привабливим для зловмисників. Серед основних вразливостей банківського сектору до відмивання коштів можна виділити:

- використання складних та багаторівневих фінансових операцій, що ускладнює виявлення незаконної діяльності;
- недостатня глибина процедур ідентифікації клієнтів, особливо у випадках з фіктивними компаніями або підставними особами;
- обмеженість у доступі до інформації про бенефіціарних власників;
- слабка інтеграція з міжнародними інформаційними системами та реєстрами [1].

Найбільш поширені методи легалізації доходів у банківській сфері:

1. Структурування транзакцій (smurfing): полягає у розділенні великих сум готівки на низку менших операцій, які не досягають порогових значень для обов'язкового фінансового моніторингу.
2. Використання підставних осіб або компаній: відкриття рахунків на ім'я третіх осіб або фірм-«оболонок» з метою маскування реального походження та одержувача коштів.
3. Використання офшорних банків та юрисдикцій з низьким рівнем фінансової прозорості: переведення коштів через низку міжнародних рахунків для ускладнення їхнього відстеження.
4. Надання «фіктивних» позик: легалізація коштів шляхом оформлення підроблених договорів позики та повернення коштів під виглядом законної операції.

В Україні систему протидії відмиванню коштів регулює Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом» [2]. Відповідальні органи – Державна служба фінансового моніторингу, НБУ, Національна поліція, СБУ. У рамках банківської системи діють правила KYC (know your customer), обов'язкова ідентифікація клієнтів, фільтрація та аналіз операцій, формування підозрілих повідомлень.

На міжнародному рівні головним орієнтиром є рекомендації FATF [3]. Україна співпрацює з MONEYVAL, поступово імплементуючи міжнародні стандарти. Проте попри певні досягнення у цій сфері варто акцентувати на таких проблемах, як:

- формалізований підхід до оцінки ризиків у багатьох банках;
- недостатнє технічне оснащення для автоматичного виявлення підозрілих транзакцій;
- обмежена взаємодія між банками та державними органами [1].

Для підвищення ефективності протидії легалізації злочинних коштів у банківському секторі доцільно впровадити наступні заходи:

1. Розширити повноваження та функціонал служб фінансового моніторингу у банках.
2. Впровадити штучний інтелект для аналізу транзакцій та виявлення аномалій.
3. Поглибити перевірку клієнтів з високим рівнем ризику (впровадити розширену перевірку – enhanced due diligence).
4. Забезпечити повноцінну інтеграцію з міжнародними реєстрами та базами даних (в т.ч. FATF, Egmont Group).
5. Ініціювати зміни до законодавства щодо прозорості власності, зокрема, розкриття бенефіціарів юридичних осіб.

Банківський сектор є одним з найбільш вразливих до процесів відмивання коштів. Його центральне положення у фінансовій системі, широкий спектр послуг, що надаються, значний обіг коштів та постійний розвиток фінансових технологій створюють численні можливості для зловживань. Злочинці активно використовують банківську систему як канал для легалізації доходів, отриманих злочинним шляхом, особливо через механізми структурованих переказів, використання фіктивних компаній, транскордонних операцій та підроблених документів.

Дослідження показало, що найбільш поширеними схемами відмивання коштів у банківському секторі є: дроблення великих сум готівки з метою уникнення порогового контролю, використання підставних осіб і компаній-оболонок, а також використання офшорних юрисдикцій для розриву ланцюга відстеження

походження коштів. Ці схеми демонструють як гнучкість злочинців, так і існуючі прогалини у фінансовому контролі (табл. 1).

Таблиця 1

Основні типові схеми відмивання коштів у банківському секторі

№	Типова схема	Опис
1	Дроблення операцій (smurfing)	Розподіл великої суми на дрібні транзакції для уникнення контролю.
2	Фіктивні компанії	Використання компаній-оболонок для переведення коштів.
3	Офшорні перекази	Переведення коштів через юрисдикції з низьким контролем.

Попри наявність нормативно-правової бази в Україні, що відповідає основним міжнародним стандартам, зокрема рекомендаціям FATF, існує низка проблем у практичній реалізації механізмів протидії [3]. Основними з них є формальний підхід до ідентифікації клієнтів, недосконаліть ризик-орієнтованого підходу, недостатній рівень технічної автоматизації процесів моніторингу та слабка взаємодія між суб'єктами фінансового моніторингу й державними органами.

Зарубіжний досвід свідчить, що для подолання цих викликів та мінімізації ризиків відмивання коштів у банківському секторі застосовують комплекс заходів. Зокрема, впровадження сучасних аналітичних технологій на базі штучного інтелекту для виявлення аномалій у транзакціях, посилення процедур KYC та EDD, удосконалення законодавчої бази щодо прозорості бенефіціарної власності, а також розширення міжнародної співпраці (табл. 2).

Таблиця 2

Порівняння національного та міжнародного рівня боротьби з відмиванням коштів

Критерій	Національний рівень (Україна)	Міжнародний рівень (FATF, ЄС, GAFILAT)
Регулювання	Закон України «Про запобігання та протидію легалізації доходів» [4]	Рекомендації FATF, Директиви ЄС
Контроль	Держфінмоніторинг, НБУ	Egmont Group, MONEYVAL
Інструменти	KYC, STR, ризик-орієнтований підхід	AML-системи, міжнародна співпраця

Таким чином, успішна протидія відмиванню коштів у банківському секторі можлива лише за умов ефективної координації між державними органами, фінансовими установами, міжнародними партнерами та технологічними провайдерами. Впровадження системного, проактивного та інтегрованого підходу дозволить не лише зміцнити фінансову безпеку країни, а й підвищити довіру до банківської системи як інструменту прозорого економічного розвитку.

Проведений аналіз свідчить, що банківський сектор України є вразливим до відмивання коштів через свою високу операційну інтенсивність, різноманітність фінансових продуктів і слабкі місцеві механізми контролю. Основні схеми легалізації – цедроблення транзакцій (smurfing), використання підставних компаній, офшорні перекази та «фіктивне» кредитування — демонструють, як гнучко адаптуються зловмисники до чинного національного та міжнародного законодавства, уникаючи виявлення. Незважаючи на те, що в Україні запроваджено систему KYC, STR і ризик-орієнтований підхід згідно із Законом України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом» та рекомендаціями FATF, на практиці спостерігаються формалізованість процесів, недостатня автоматизація та обмежена взаємодія між фінансовими установами й держорганами.

Для підвищення ефективності протидії відмиванню коштів доцільно реалізувати комплекс заходів: розширити функціонал внутрішніх підрозділів фінмоніторингу в банках; впровадити аналітичні системи на базі штучного інтелекту для виявлення аномалій; застосувати розширену перевірку клієнтів з високим рівнем ризику (Enhanced Due Diligence); забезпечити інтеграцію з міжнародними реєстрами (FATF, Egmont Group) [4]; а також удосконалити законодавство щодо прозорості бенефіціарної власності. Лише посилена координація між державними органами, фінансовими установами, технологічними провайдерами та міжнародними партнерами зможе сформувати проактивну, системну і стійку модель боротьби з відмиванням коштів, що сприятиме зміцненню фінансової безпеки України та підвищенню довіри до банківської системи.

Список використаних джерел:

1. Zaburanna L., Nedilska L., Abramova, I., Kurovska, N., Martynuk G. The Development of the Banking System in Conditions of Destructive Impact of Internal and External Factors. Scientific Horizons. 3(88), 2020. pp. 7-18. URL.: https://doi.org/10.33249/2663-2144-2020-88-3-7-18

2. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом». URL.: https://zakon.rada.gov.ua/laws/show/1702-18 (дата звернення: 10.04.2025).

3. Financial Action Task Force. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris : FATF, 2012. 56 p.

4. Egmont Group. The Egmont Group Charter [Електронний ресурс]. – Режим доступу: https://egmontgroup.org/en/content/egmont-group-charter (дата звернення: 11.05.2025).

УДК 342:351.86(477)

Горєлий С.С., аспірант кафедри публічного управління та адміністрування
Хмельницький університет управління та права імені Леоніда Юзькова

СУЧАСНІ ПІДХОДИ ДО СУТНОСТІ ПОНЯТТЯ «НАЦІОНАЛЬНА БЕЗПЕКА»

У сучасному світі гарантування національної безпеки є дедалі складнішим завданням через зростаючу кількість різноманітних загроз, серед яких тероризм, кібернетичні атаки, гібридні війни, економічні та фінансові потрясіння, а також пандемії. Ефективна система національної безпеки вимагає налагодженої взаємодії та співробітництва як між державними структурами, так і між державою та суспільством.

З огляду на стрімке зростання глобальної нестабільності та появу нових, нетрадиційних загроз, питання національної безпеки набуває особливої гостроти та актуальності. Традиційні підходи вже не повною мірою відповідають сучасним реаліям, що вимагає переосмислення стратегій та інструментів для ефективного захисту національних інтересів. Сьогодні надзвичайно важливо враховувати взаємопов'язаність різних сфер безпеки – від військової до економічної, інформаційної й екологічної – та налагоджувати гнучку систему реагування на комплексні виклики.

Забезпечення національної безпеки в різних сферах життя є центральним завданням для урядів, міждержавних структур і громадських ініціатив. Протягом багатьох років українські науковці в різних галузях активно обговорювали питання безпеки. Однак, у вітчизняному науковому дискурсі нерідко спостерігалася термінологічна плутанина, коли поняття «національна безпека» фактично замінювалося «міжнародною безпекою», «державною безпекою» (як безпекою саме держави) або загальним терміном «безпека». Для належного дослідження цієї важливої проблематики необхідно здійснити всебічне розкриття сутності та змісту «національної безпеки», враховуючи всі її специфічні ознаки.

Насамперед слід визначитися з суттю поняття «безпека». Великий тлумачний словник сучасної української мови визначає безпеку у загальновживаному розумінні цього слова як «стан, коли комусь, чомусь ніщо не загрожує» [1]. Оксфордський тлумачний словник говорить: безпека – це «1) свобода чи захист від небезпеки чи тривоги; 2) заходи, вжиті задля забезпечення безпеки країни, особи, цінності» [2]. Виходячи з цього, більшість визначень поняття «національна безпека» характеризується через стан або стан об'єкта безпеки, коли для нього відсутня небезпека, тобто змін властивостей у гірший бік, або стан, що забезпечує достатню економічну чи військову міць нації для опору загрозам її існування, що виходять як з інших країн, так і зсередини своєї країни.

Нами систематизовано погляди зарубіжних та вітчизняних вчених, а також офіційні визначення поняття «національна безпека», які закріплені у нормативно-правових та інших документах (табл. 1).

Таблиця 1

Визначення поняття «національна безпека»

Автор, джерело	Визначення
Власюк О.С.	Національна безпека - система державно-правових і суспільних гарантій стабільності життєдіяльності та розвитку українського народу загалом та кожного громадянина зокрема, захист їхніх базових цінностей і законних інтересів, джерел духовного та матеріального розвитку від можливих реальних і потенційних, внутрішніх та зовнішніх загроз.
Ліпкан В.А., Ліпкан О.С.	Національна безпека - це своєрідна сфера існування людини, нації, держави, культури, традицій, звичаїв, ресурсів, що не лише міцно пов'язує людей між собою, а й єднає їх із історичною спадщиною та навколишнім середовищем.
Політична енциклопедія	Національна безпека - це здатність країни зберігати цілісність, суверенітет, політичні, економічні, соціальні та інші основи суспільного життя й виступати як самостійний суб'єкт міжнародних відносин.
Закон України «Про національну безпеку України»	Національна безпека України - захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз.
Браун Г.	Національна безпека – це здатність зберігати територію, підтримувати економічні відносини з іншими країнами світу, на різних рівнях захищати від зовнішнього негативного впливу свої інститути та систему управління, контролювати свої кордони.
Фахівці Європейського Центру з вивчення питань безпеки ім. Дж. К. Маршалла	Національна безпека – термін, який включає поняття національної оборони та характер відносин з іншими країнами (зокрема, умови, які створюються військовою чи оборонною перевагою над будь якою країною (групою країн) або вигідною позицією в міжнародних відносинах).

Примітка. Систематизовано автором на основі [3, с. 25; 4, с.10; 5-8].

Виходячи з детального аналізу сутності та змісту поняття «національна безпека» пропонуємо виділити наступні підходи:

1. Державоцентричний підхід. Цей підхід розглядає державу як центральний об'єкт і головного гаранта національної безпеки. З цієї точки зору, національна безпека визначається як стан захищеності життєво важливих інтересів держави від внутрішніх і зовнішніх загроз. Основними характеристиками

державоцентричного підходу є:

пріоритет держави: Державні інтереси ставляться вище за інтереси особистості та суспільства. Забезпечення безпеки держави розглядається як необхідна умова для забезпечення безпеки її громадян;

сильна роль державних інститутів. Головна відповідальність за забезпечення національної безпеки покладається на державні органи влади, такі як збройні сили, спецслужби, правоохоронні органи та інші;

акцент на зовнішніх загрозах. Традиційно основна увага приділяється захисту від зовнішньої агресії, військових конфліктів, міжнародного тероризму та інших загроз, що походять з-за меж держави;

суверенітет і територіальна цілісність. Захист державного суверенітету, незалежності та територіальної цілісності є ключовими елементами національної безпеки в рамках цього підходу;

державний інтерес. Визначення національної безпеки тісно пов'язане з поняттям державного інтересу, який включає збереження політичної стабільності, економічного процвітання, культурної ідентичності та міжнародного впливу держави.

Однак, цей підхід також має свої обмеження та критику. Зокрема, він може недооцінювати важливість безпеки особистості та суспільства, а також внутрішні загрози, такі як корупція, соціальна нерівність, порушення прав людини тощо. Крім того, надмірний акцент на державі може призвести до обмеження громадянських свобод в ім'я безпеки.

В контексті сучасних реалії в Україні, державоцентричний підхід є особливо актуальним в умовах триваючої російської агресії та необхідності захисту суверенітету й територіальної цілісності. Водночас, важливо враховувати й інші аспекти національної безпеки, включаючи економічну, енергетичну, інформаційну, екологічну та гуманітарну складові, а також забезпечувати баланс між безпекою держави та правами і свободами громадян. Варто зазначити, що сучасні концепції національної безпеки все частіше відходять від чисто державоцентричного підходу, наголошуючи на комплексному характері безпеки, що включає не лише державні, але й суспільні та особистісні аспекти. Тим не менш, держава залишається ключовим актором у забезпеченні національної безпеки, і її роль є визначальною.

2. Людиноцентричний (ліберальний) підхід. Даний підхід ставить в центр уваги людину, її права, свободи та добробут. На відміну від державоцентричного підходу, де головним об'єктом безпеки є держава, тут акцент переноситься на захист індивіда та створення умов для його всебічного розвитку.

Основніими ознаками людськоцентричного підходу є:

- пріоритет особистості. Безпека кожної людини є найвищою цінністю. Безпека держави розглядається як засіб забезпечення безпеки її громадян, а не самоціль;
- широке розуміння загроз. Загрози національній безпеці не обмежуються лише військовими або зовнішніми агресіями. Вони включають також соціально-економічні проблеми (бідність, нерівність, безробіття), порушення прав людини, екологічні катастрофи, пандемії, інформаційну дезінформацію та інші чинники, що негативно впливають на життя та розвиток людей;
- захист прав і свобод. Ключовим елементом національної безпеки є гарантування та захист основних прав і свобод людини, включаючи громадянські, політичні, економічні, соціальні та культурні права;
- верховенство права та демократія. Демократичні інститути та верховенство права розглядаються як важливі інструменти забезпечення національної безпеки, оскільки вони сприяють підзвітності влади, запобігають зловживанням і забезпечують мирне врегулювання конфліктів;
- активна роль громадянського суспільства. Забезпечення національної безпеки розглядається як спільна відповідальність держави та громадянського суспільства. Активна участь громадян у прийнятті рішень, контроль за діяльністю влади та розвиток громадських ініціатив є важливими елементами цього підходу.

Критика цього підходу часто полягає в тому, що надмірний акцент на правах особистості може послабити державу та її здатність ефективно протистояти зовнішнім загрозам. Також існує ризик того, що широке визначення загроз може розмити поняття національної безпеки та ускладнити визначення пріоритетів.

Таким чином, в сучасному світі спостерігається тенденція до інтеграції елементів як державоцентричного, так і людиноцентричного підходів у концепціях національної безпеки. Розуміння того, що безпека держави та безпека її громадян є взаємопов'язаними та взаємозалежними, стає все більш поширеним. В контексті України, особливо важливим є забезпечення безпеки кожної людини в умовах війни та післявоєнного відновлення, одночасно зміцнюючи державу для захисту від зовнішньої агресії.

Список використаних джерел:

1. Великий тлумачний словник сучасної української мови / голов. ред. В.Т. Бусел. К. ; Ірпінь : ВТФ «Перун», 2005. 1728 с.
2. Оксфордський словник англійської мови. URL: https://oxforddictionaries.com.
3. Власюк О.С. Національна безпека України: еволюція проблем внутрішньої політики: Вибр. наук. праці. К.: НІСД, 2016. 528 с.
4. Ліпкан В.А., Ліпкан О.С. Національна і міжнародна безпека у визначеннях та поняттях : словник. Вид. 2-ге, доповн. і переробл. Київ, 2008. 400 с.
5. Політична енциклопедія. Редкол.: Ю. Левенець (голова), Ю. Шаповал (заст. голови) та ін. К.: Парламентське видавництво, 2011. 808 с.
6. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII
7. Brown H. Thinking About National Security. Defense and Foreign Policy in a Dangerous World., 1983. P. 4.
8. Глосарій термінів. Гарміш-Партенкірхен Європ. Центр вивчення пит. безпеки ім. Дж.Д. Маршалла.

УДК 327

Камінський І.О., студент 2 курсу
Науковий керівник: Попович Н.В., асистент кафедри національної безпеки, публічного управління та адміністрування
Державний університет «Житомирська політехніка»

ТЕРОРИЗМ ТА НЕЗАКОННИЙ ОБІГ ЗБРОЇ ЯК ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ КРАЇНИ

Теоретичне осмислення проблематики тероризму та незаконного обігу зброї вимагає розуміння їхнього взаємозв'язку та взаємовпливу. Незаконний обіг зброї створює матеріально-технічні передумови для терористичної діяльності, забезпечуючи терористичні групи засобами здійснення насильницьких дій. Водночас, терористичні організації часто залучені до незаконного обігу зброї як джерела фінансування своєї діяльності, що створює замкнений цикл підтримки цих негативних явищ. Теоретичний аналіз взаємозв'язку тероризму та незаконного обігу зброї дозволяє розробити комплексні підходи до протидії цим явищам, враховуючи їхню взаємообумовленість та спільні причини.

В Україні окремі питання тероризму та незаконного обігу зброї досліджували Шаблистий В.В., Симоненко Н.О., Хоменко А.О., Сорока О.А., Яценко С.В., Марков М.М., Євтушенко С.В., Зима Д.С., Титаренко Ю.М., однак окремі аспекти даної теми потребують деталізації та уточнення.

Боротьба з тероризмом в умовах національних безпекових викликів вимагає впровадження інтегрованого підходу, що поєднує правові, організаційні, інформаційні та соціально-економічні інструменти. Концептуальною основою такого підходу має бути розуміння тероризму як комплексного феномену, що потребує багаторівневої системи протидії. Це передбачає не лише реагування на конкретні терористичні акти, але й профілактику радикалізації, моніторинг потенційних терористичних загроз, контроль за обігом зброї та вибухових речовин.

Окремо варто відзначити технологічні види незаконного обігу зброї, що з’явилися відносно нещодавно. Розвиток технологій 3D-друку створює можливості для виготовлення зброї в домашніх умовах без спеціалізованого обладнання, що суттєво ускладнює контроль за виробництвом зброї. Пластикова зброя, виготовлена за допомогою 3D-принтерів, становить особливу небезпеку, оскільки може не фіксуватися стандартними детекторами металу на пунктах безпеки. Крім того, розвиток даркнету та використання криптовалют для анонімних розрахунків створюють нові канали для нелегальної торгівлі зброєю, що важко відстежуються традиційними правоохоронними методами.

Специфічною рисою терористичної загрози для України є її взаємозв'язок із незаконним обігом зброї, що створює сприятливі умови для здійснення терористичної діяльності. Куций Я.А. підкреслює, що доступність вогнепальної зброї, боєприпасів та вибухових речовин через нелегальні канали постачання суттєво підвищує терористичні ризики та створює додаткові виклики для системи національної безпеки [1, с. 25]. За даними Офісу Генерального прокурора України, протягом 2024 року було зареєстровано значну кількість кримінальних правопорушень, пов'язаних із незаконним обігом зброї, що створює підґрунтя для терористичної діяльності. Кучер В.М. та Василевич В.В. зазначають, що контроль за обігом зброї є важливим елементом системи протидії тероризму, оскільки обмежує доступ терористичних угруповань до засобів здійснення терористичних актів [2, с. 32]. Особливістю терористичної загрози для України є її зв'язок з інформаційно-психологічними операціями, спрямованими на дестабілізацію суспільно-політичної ситуації та підрив довіри до державних інститутів. Тероризм як загроза національній безпеці України має динамічний характер, що вимагає постійного моніторингу та адаптації системи протидії до нових викликів та загроз.

Таким чином, тероризм як загроза національній безпеці України потребує глибокого теоретичного осмислення та розробки ефективних механізмів протидії, що враховують динамічний характер терористичних загроз та їх взаємозв’язок з іншими деструктивними явищами. Розуміння сутності та видів тероризму створює підґрунтя для формування комплексної державної політики у сфері забезпечення антитерористичної безпеки, спрямованої на захист національних інтересів України та забезпечення безпеки її громадян.

Список використаних джерел:

1)Куций Я. А. Незаконний обіг зброї в Україні: поняття та проблеми вирішення: дис. Вінниця: ВНТУ, 2019. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/27317/7695.pdf

2)Кучер В. М., Василевич В. В. Запобігання незаконному заволодінню вогнепальною зброєю, бойовими припасами, вибуховими речовинами. Київ, 2022. URL:https://elar.navs.edu.ua/server/api/core/bitstreams/c3801af7-fcba-4eea-8350-2249ce1e26ea/content

УДК 327

Лаврієнко М.М., здобувачка вищої освіти
на бакалаврському рівні юридичного факультету
Лалуєва Н.М., асистент кафедри публічного управління та адміністрування
Хмельницький університет управління та права ім. Леоніда Юзькова

ІНФОРМАЦІЙНА БЕЗПЕКА В ПЕРІОД ДІЇ ВОЄННОГО СТАНУ

У сучасному світі інформація стала одним із ключових ресурсів, а її безпека – критичним чинником національної стійкості, особливо в умовах воєнного стану. З початком повномасштабної агресії російської федерації проти України інформаційна безпека набула особливого значення. Поширення фейків, кібератаки, маніпуляції громадською думкою та втручання в інформаційний простір країни стали складовими гібридної війни. Саме тому дослідження аспектів інформаційної безпеки під час воєнного стану є актуальним і необхідним для збереження суверенітету, стабільності та цілісності України.

Варто зазначити, що поняття «інформаційна безпека» трактується науковцями по-різному. Зокрема, В.С. Цимбалюк розглядає її як стан захищеності національних інтересів у сфері інформації [1]. У свою чергу, Л.О. Кочубей вважає, що інформаційна безпека характеризує рівень захисту важливих інтересів держави, суспільства та особи, а також їхню здатність ефективно використовувати інформаційні ресурси в сучасних умовах [2]. На нашу думку, інформаційна безпека охоплює належний рівень інформаційної культури кожної особистості, здатність держави забезпечити сприятливі умови для повноцінного доступу до інформації та її використання без ризику впливу шкідливих факторів. Вона також передбачає гарантії розвитку інформаційного простору відповідно до потреб людини та захист від потенційних загроз в інформаційній сфері.

З метою посилення інформаційної безпеки в Україні 25 лютого 2017 року Указом Президента було ухвалено «Доктрину інформаційної безпеки України» [3]. У період воєнного стану, 18 березня 2022 року, Рада національної безпеки і оборони прийняла рішення «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», де підкреслюється, що впровадження єдиної інформаційної політики є ключовим аспектом національної безпеки [4]. Зараз в Україні функціонує Центр протидії дезінформації при РНБО, який через офіційний сайт інформує громадськість про актуальні події та питання, пов'язані з інформаційною безпекою. Інформаційна безпека відіграє ключову роль під час воєнного стану, оскільки спотворена або неправдива інформація може спричинити паніку серед населення, послабити довіру до влади та знизити авторитет військово-політичного керівництва. Усе це негативно позначається на ефективності бойових дій та може зашкодити досягненню стратегічних цілей. Тому протидія поширенню шкідливої інформації є вкрай важливою для успішного ведення воєнного конфлікту.

Головними шляхами поширення недостовірної інформації в умовах війни є соціальні мережі. Окрім того, у сфері інформаційної безпеки значну загрозу становлять чутки — недостовірні повідомлення в різних формах, які залишаються впливовим засобом комунікації навіть у добу цифрових технологій. З появою Інтернету вони лише посилили свій вплив, набравши «віртуальної» форми. Висока швидкість розповсюдження інформації в мережі та анонімність спілкування створюють сприятливе середовище для поширення чуток. Окремою загрозою в контексті інформаційної безпеки є поширення фейків — свідомо вигаданої інформації, що не має під собою жодних реальних підстав. Такі повідомлення завжди комусь вигідні: «сенсаційні» новини приносять більше переглядів, а емоційні теми на кшталт «зради» чи «перемоги» часто використовуються у політичній пропаганді. Фейки базуються на неправді, маніпуляціях та спотворенні реальності.

Потрібно зауважити, що ефективна протидія неправдивій, викривленій і неперевіреній інформації під час війни базується, насамперед, на підвищенні рівня медіаграмотності громадян. Це дає змогу не лише захищати себе від інформаційних атак, а й сприяти збереженню інформаційної безпеки держави. російська федерація активно веде інформаційну війну, намагаючись через пропаганду розколоти українське суспільство та дискредитувати його в очах міжнародної спільноти. Проросійські наративи навмисно поширюються для того, щоб вдарити по вразливих точках, відкритих війною. У зв'язку з цим важливо навчитися мислити критично: аналізувати, яку мету переслідує певний контент, хто його створив і яку шкоду він може нести. Такий підхід допомагає уникати пасток маніпуляцій і не поширювати шкідливу інформацію далі. Додатково, надзвичайно важливим є регулярне й об'єктивне інформування громадян через офіційні джерела, зокрема державні ЗМІ та звернення посадовців. Це сприяє формуванню довіри, викриттю фейків і зменшенню впливу чуток, особливо в умовах війни.

Список використаних джерел:

1. Цимбалюк, В.С. 2014. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики, Адміністративне право і процес 22–30 с.

2. Кочубей, Л.О. 2015. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). Наукові записки Інституту політичних і етнонаціональних досліджень імені І.Ф. Кураса 220-237 с.

3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017 URL: https://zakon.rada.gov.ua/go/47/2017 (дата звернення: 12.04.2025).

УДК 327

Олійник А.М., здобувачка вищої освіти
на бакалаврському рівні юридичного факультету
Лалуєва Н.М., асистент кафедри публічного управління та адміністрування
Хмельницький університет управління та права ім. Леоніда Юзькова

ІНФОРМАЦІЙНА ВІЙНА В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ: ВИКЛИКИ ТА ПРОТИДІЯ

У зв'язку з початком збройної агресії російської федерації 24 лютого 2022 року на всій території України було запроваджено режим воєнного стану [1]. Воєнні дії, масовані атаки, а також цілеспрямоване поширення фейкової інформації мають на меті посилення страху й панічних настроїв у суспільстві та діють як інструмент інформаційної війни. Така діяльність негативно впливає на стабільність політичної, соціальної та економічної ситуації в Україні. Сучасні реалії змушують нас по-новому поглянути на питання безпеки, адже війна відкрила новий фронт — інформаційний. Щоденно ми стаємо свідками того, як інформаційні атаки впливають не лише на окремих людей, але й на цілі спільноти, а іноді такому впливу піддаються й зарубіжні держави. Йдеться не просто про новини чи повідомлення, а про цілеспрямовані спроби змінити свідомість, зламати віру, викликати сумніви й страх. У таких умовах надзвичайно важливо не лише розпізнавати ці загрози, а й навчитися їм протистояти.

Масові інформаційні атаки, діяльність ботів і поширення фейків стали основними викликами інформаційної війни, спрямованими на дезорієнтацію суспільства, провокування страху, маніпулювання свідомістю та створення паніки. До цього переліку варто віднести й спеціально створені інформаційні ресурси, що впливають на мислення громадян, стимулюючи їх до сприйняття викривленої та неправдивої інформації [2, с. 34].

У цьому контексті варто зазначити твердження О.І. Косілової, яка приходить до висновку, що для запобігання та протидії загрозам в інформаційному просторі країни важливо на державному рівні систематично розробляти нові та вдосконалювати чи модернізувати чинні нормативно-правові акти у сфері інформаційного захисту. Війна дуже швидко розвивається, тому наша країна повинна у такому ж темпі вдосконалювати правову базу [3, с. 25].

В умовах воєнного стану органи публічної влади мають забезпечувати високий рівень інформаційної взаємодії не лише з громадянами України, а й із представниками цивілізованого світу. Публічні звернення Президента України, представників уряду, дипломатів та інших посадовців перед парламентами іноземних держав, міжнародними організаціями або зарубіжними медіа мають бути виваженими, заснованими виключно на достовірних фактах і чітких заявах [4, с. 44].

З вищевикладеного можна дійти висновку, що під час дії воєнного стану на території держави питання інформаційної безпеки набуває надзвичайного значення, оскільки стає питанням не лише окремої людини, а й усього суспільства та держави. Інформаційна безпека безпосередньо пов'язана з правами та свободами громадян, головними аспектами якої є збереження цілісності даних, забезпечення доступності, конфіденційності та достовірності інформації [5].

Таким чином, в умовах воєнного стану в Україні інформаційна безпека стає ключовим елементом національної безпеки. Ефективна протидія інформаційним загрозам вимагає комплексного підходу, що включає правове регулювання, розвиток технологічних рішень та підвищення інформаційної грамотності населення.

Список використаних джерел:

1. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 № 64/2022 URL: https://zakon.rada.gov.ua/go/64/2022 (дата звернення: 16.05.2025).

2. Панченко О. А., Панченко Л. В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві // Правова інформатика. 2015. № 2(46). С. 32–38. URL: https://ippi.org.ua/panchenko-oa-panchenko-lv-informatsiina-bezpeka-ta-informatsiina-kultura-v-suchasnomu-informatsiinom (дата звернення: 16.05.2025).

3. Косілова О. І. Інформаційна безпека України в умовах глобалізації // Правова інформатика. 2010. № 3(27). С. 20–28. URL: https://ippi.org.ua/oi-kosilova-informatsiina-bezpeka-ukraini-v-umovakh-globalizatsii.

4. Ніколаєць Ю. О. Державна інформаційна політика України в умовах повномасштабного воєнного вторгнення Російської Федерації: суспільно-мобілізаційний потенціал і ефективність // Політичні дослідження. 2024. № 1(7). С. 42–67. URL: https://ipiend.gov.ua/wp-content/uploads/2024/05/3_Nikolaiets.pdf (дата звернення: 16.05.2025).

5. Права і свободи громадян в умовах воєнного стану // WikiLegalAid. URL: https://wiki.legalaid.gov.ua/index.php/Права_і_свободи_громадян_в_умовах_воєнного_стану.

УДК 355.1:364-7 (477)

Помаза-Пономаренко А.Л., д.держ.упр., с.д.,
завідувач науково-дослідної лабораторії з дослідження
проблем управління у сфері цивільного захисту
Національний університет цивільного захисту України, м. Харків
Тарадуда Д.В., к.т.н., доцент, доцент кафедри ліквідації
наслідків надзвичайних ситуацій інституту післядипломної освіти
Львівський державний університет безпеки життєдіяльності, м. Львів

СОЦІАЛЬНИЙ СУПРОВІД ЯК НАПРЯМ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Через повномасштабну агресію рф в Україні стрімко знижується рівень її національної, і що важливо, соціальної безпеки. Свідченням цього є збільшення кількості осіб з інвалідністю серед українців, значний відтік працездатного населення за кордон, демографічна криза та ін. Відтак, перед Україною стоїть завдання щодо підвищення рівня національної безпеки крізь призму вдосконалення соціальної політики, зокрема активне впровадження механізму соціального супроводу. Власне, такий супровід надзвичайно необхідний для військових і осіб МВС, які отримали поранення, а також для членів їхніх сімей.

Варто відзначити, що соціальний супровід військовослужбовців й осіб у системі Міністерства внутрішніх справ (далі – МВС) є важливим аспектом забезпечення прав та законних інтересів як співробітників, так і громадян, які перебувають у зоні відповідальності відомства [1]. Ефективне управління цими процесами вимагає комплексного підходу, що враховує специфіку діяльності МВС і потреби різних категорій осіб [3]. Зважаючи на наявні моделі соціального захисту осіб [там само], основними напрямками соціального супроводу співробітників МВС можуть бути визнані такі:

1. Соціальний захист:

– забезпечення гарантій та компенсацій у разі поранення, захворювання або загибелі співробітників під час виконання службових обов'язків;

– надання психологічної підтримки та реабілітації співробітникам, які пережили стрес;

– соціальна адаптація та працевлаштування співробітників, які звільнилися з органів внутрішніх справ.

2. Соціальний супровід осіб, які перебувають під вартою (забезпечення належних умов утримання та медичного обслуговування; надання правової допомоги та психологічної підтримки; соціальна адаптація та реінтеграція осіб, які звільнилися з місць позбавлення волі).

3. Соціальний супровід постраждалих від воєнних злочинів (надання психологічної підтримки та правової допомоги; забезпечення захисту прав та законних інтересів; соціальна реабілітація та відновлення).

4. Соціальний супровід осіб та їх сімей, які перебувають у складних життєвих обставинах (надання допомоги у вирішенні соціально-побутових проблем, забезпечення доступу до соціальних послуг і пільг, соціальна адаптація й інтеграція та ін.).

Слід зазначити, що принципами управління процесами соціального супроводу осіб у системі МВС є такі: 1) законність (передбачає, що діяльність у сфері соціального супроводу має здійснюватися відповідно до чинного законодавства); 2) гуманність (необхідно поважати права та гідність кожної особи, а також осіб у системі МВС, які потребують соціального супроводу); 3) індивідуалізації, що вимагає здійснення соціального супроводу з урахуванням індивідуальних потреб та особливостей кожної особи, яка виконує службові обов’язки в системі МВС; 4) комплексність (необхідно забезпечити упровадження комплексного підходу до вирішення проблем, що потребують соціального супроводу осіб у системі МВС); 5) налагодження дієвої міжвідомчої співпраці (необхідно налагодити ефективну співпрацю між МВС й організаціями, які надають соціальні послуги (Міністерством соціальної політики, Міністерством охорони здоров'я та ін.)). Підкреслимо, що важливо дієво взаємодіяти з Національною соціальною сервісною службою України, нею зреалізовується експериментальний проєкт соціального супроводу військовослужбовців до жовтня 2025 р. [4].

Згідно з Наказом МВС від 06.11.2023 №895 «Про затвердження Положення про функціональну підсистему «Соціально-правовий захист постраждалих та членів їх сімей» єдиної інформаційної системи» [2] створено ФП СПЗ – інформаційно-комунікаційну систему, яка представляє собою сукупність інформаційних, технічних і програмних засобів, які автоматизують централізовану обробку відомостей про військовослужбовців Національної гвардії України, Держприкордонслужби, осіб рядового і начальницького складу служби цивільного захисту ДСНС, поліцейських, які загинули (померли), зникли безвісти, захоплені в полон або заручниками, інтерновані в нейтральних державах, звільнені з полону, отримали поранення внаслідок збройної агресії рф проти України, та членів їх сімей. Ця система дозволяє забезпечити соціально-правовий захист зазначених осіб, тобто комплекс заходів, спрямованих на надання

послуг, необхідних для задоволення основних потреб, медичного забезпечення, психологічного супроводу, забезпечення реалізації соціальних гарантій та виплат постраждалим та членам їх сімей.

Власником та розпорядником ФП СПЗ є держава в особі Міністерства внутрішніх справ України. Відомості вносяться до ФП СПЗ українською мовою на підставі даних відповідних підрозділів соціально-гуманітарного забезпечення (соціального супроводу), морально-психологічного забезпечення, кадрового забезпечення, медичного забезпечення, бухгалтерської служби суб'єктів ФП СПЗ та інших документів, які містять інформацію про інформаційні об'єкти ФП СПЗ.

У той же час, механізм управління процесами соціального супроводу осіб в системі МВС потребує розвитку, що можливий у таких напрямках: 1) розвиток нормативно-правової бази (необхідно вдосконалити законодавство у сфері соціального супроводу, ураховуючи сучасні виклики, зумовлені повномасштабною агресію рф); 2) підвищення кваліфікації кадрів відділень (управлінь, секторів та ін.) соціального супроводу, удосконалення інформаціної діяльності таких відділень, управлінь, секторів при медичних закладах, адже про них мало обізнане населення, яке звертається до цих закладів ; 3) відтак, набуває важливості активне та виважене впровадження інформаційних технологій з метою надання вчасної допомоги в межах функціонуючої служби соціального супроводу; 4) активне залучення громадських організацій (зокрема, волонтерських) із метою підвищення результативності соціального супроводу осіб у системі МВС, зокрема, до надання соціальних послуг і контролю за їх якістю.

Список використаних джерел:

1. Домбровська С., Помаза-Пономаренко А., Порока С., Сємілєтов О. Напрямки розвитку державного управління у сфері охорони громадського порядку : монографія. Харків: НУЦЗУ, 2024. 272 с.

2. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws.

3. Помаза-Пономаренко А.Л. Соціальний розвиток і безпека регіонів: державно-управлінські аспекти : монографія. Харків: Видавництво «Діса плюс», 2017. 270 с.

4. Соціальний супровід військовослужбовців та членів їх сімей у військових частинах (підрозділах). URL: https://nssu.gov.ua/eksperementalni-proiekty/sotsialnyi-suprovid-viiskovosluzhbovtsiv-ta-chleniv-ikh-simei-u-viiskovykh-chastynakh-pidrozdilakh-zbroinykh-syl.

УДК 327

Рафальський Є.О., здобувач вищої освіти другого рівня вищої освіти,
Науковий керівник: Клименко І.В., к.е.н., доцент кафедри національної безпеки, публічного управління та адміністрування
Державний університет «Житомирська політехніка»

СУЧАСНІ ТЕОРІЇ ЦИВІЛЬНОЇ БЕЗПЕКИ: СВІТ ТА УКРАЇНА

Загострення безпекової ситуації в Європі після початку повномасштабної агресії Російської Федерації проти України призвело до трансформації національних та міжнародних підходів до захисту цивільного населення. Війна, що супроводжується інформаційним тиском, соціальною нестабільністю, руйнуванням інфраструктури та порушенням базових прав, вплинула на переосмислення форм та механізмів захисту громадянського простору. В умовах гібридних викликів зросла потреба у переоцінці функціонування структур цивільної безпеки. Середовище загроз набуло комплексного характеру: поєднання воєнної, інформаційної, кібернетичної, гуманітарної безпеки більше не дозволяє обмежуватися лише мілітарною логікою захисту.

Поняття цивільної безпеки варіюється залежно від нормативно-правової традиції. У міжнародному дискурсі воно охоплює захист цивільних осіб у разі збройного конфлікту, забезпечення прав людини, готовність до надзвичайних ситуацій, протидію тероризму, а також координацію між силовими та несиловими структурами. У національному контексті, зокрема в Україні, в умовах воєнного стану цивільна безпека включає захист населення в умовах бойових дій, підтримку функціонування критичної інфраструктури, евакуаційні процеси, інформування населення та стабілізацію внутрішнього правопорядку [1, с. 44–45].

У світовій науковій традиції переважає кілька базових концептуальних підходів до трактування безпеки. Ліберальні підходи акцентують на інституційному регулюванні, пріоритеті прав людини та колективній відповідальності. Відповідно до цієї логіки, безпека розглядається як продукт взаємодії демократичних інститутів, ефективного врядування та відкритості суспільства до контролю. У таких моделях перевага надається превентивним стратегіям та розвитку гуманітарного сектору.

Конструктивістські підходи формують безпекові уявлення через призму соціальних конструкцій, у яких значення загроз не є об'єктивними даними, а виникають у результаті сприйняття та інтерпретацій. Відповідно, реагування залежить від комунікаційних механізмів, довіри до влади та символічного капіталу інституцій.

Сучасні теорії зосереджуються на нерівностях доступу до ресурсів безпеки, впливу глобальних політичних структур на локальні спільноти, а також деколоніальних підходів до охорони громадянської середовища. Автори цих підходів заперечують одновимірність безпеки як захисту держави та надають перевагу соціальній справедливості, рівному доступу до безпечної середовища та демілітаризації простору [2, с. 180-181].

Узагальнення теоретичних моделей призвело до формування концепції людської безпеки, що стала предметом уваги міжнародних організацій. Згідно з цим баченням, безпека визначається як свобода від страху, злиднів, соціальної маргіналізації. У фокусі опиняються індивідуальні потреби, зокрема доступ до медицини, їжі, житла, психологічної підтримки, освіти, а не тільки захисту від збройного насильства. Такий підхід активно використовують ООН у гуманітарних операціях і в політиці розвитку.

У структурі НАТО та Європейського Союзу сформовані політики цивільної безпеки, орієнтовані на багаторівневу координацію між силовими, цивільними та волонтерськими структурами. Зокрема, ЄС активно впроваджує концепцію «стійкості суспільства» через програми підтримки демократичних інституцій, реформу сектору безпеки, розвиток місцевого самоврядування, підвищення готовності громад до надзвичайних подій [2, с. 182].

Гібридна війна змінила уявлення про захист цивільного населення. Бойові дії поєднуються з інформаційними операціями, кібератаками, економічним тиском, психологічним впливом. У таких умовах значення цивільної безпеки виходити за межі протидії прямому насильству. До складу безпеки входять інформаційна стійкість, злагодженість громад, економічна підтримка та психологічна готовність до загроз [2, с. 180-182].

У практиці держав, що тривалий час перебувають у конфліктній середовищі, сформовано дієві моделі реагування. В Ізраїлі застосовується принцип інтеграції громадян до системи національного реагування, в Литві — концепція «всеохоплюючої захисту», де кожний зв'язок суспільства долучений до безпеки. У Грузії акцент зроблено на інформаційній грамотності та локальних мережах підтримки [2, с. 183].

В Україні цивільна безпека перебуває під тиском зовнішніх агресивних дій та внутрішніх соціальних викликів. До переліку загроз входить дестабілізація громадської думки, руйнування інфраструктури, високий рівень тривожності серед населення. Прифронтові регіони відчувають дефіцит ресурсів, обмеження в мобільності та потребують постійної уваги з боку державних та місцевих структур. Система

публічної безпеки в таких умовах працює у надзвичайному режимі, поєднуючи правові, гуманітарні та координаційні механізми [1, с. 45-48].

Міжнародна підтримка стала основою реформування сектору цивільної безпеки. Угода між Україною та Європейським Союзом виокремила правові рамки функціонування Консультативної місії ЄС. Місія працює над удосконаленням політики у правоохоронному секторі, зміцненням потенціалу ДСНС, модернізацією інституцій прокуратури та забезпеченням належного стандарту підготовки персоналу. Рекомендації КМЄС спрямовані на гармонізацію української безпекової політики з європейськими підходами, де пріоритет мають прозорість, відповідальність та захист прав людини [3].

Отже, цивільна безпека у світовому та національному вимірі постає як багатоелементна система, що охоплює не лише захист від фізичних загроз, а й забезпечення стабільності соціального, інформаційного та економічного середовища. У контексті гібридної війни змінюється підхід до безпеки населення: держава більше не є єдиним гарантом, залучення громадянських структур та міжнародних партнерів стає умовою стійкості.

Міжнародна практика демонструє дієвість моделей, побудованих на децентралізації реагування, розвитку місцевих ініціатив та просвітницької роботи. Україна адаптує ці підходи відповідно до власних викликів, інтегруючи рекомендації міжнародних місій та реформуючи інститути безпеки.

Правове забезпечення, ефективна комунікація між владою та населенням, підтримка на рівні ЄС та НАТО створюють умови для розвитку громадянської безпеки як сталої частини державної політики. За збереження інституційної послідовності та стратегічного бачення можливе побудування моделі, здатної протистояти багаторівневим загрозам у довготривалій перспективі.

Список використаних джерел:

1. Батраченко Т., Сухацька І. Публічна (громадська та цивільна) безпека в україні в умовах військового стану. Національні інтереси України. 2025. № 2(7). С. 43-52. URL: https://doi.org/10.52058/3041-1793-2025-2(7)-43-52.

2. Пастух І., Кришевич О., Пендюра М. Цивільна безпека в умовах гібридної війни у міжнародному вимірі. Наукові інновації та передові технології. 2023. № 14(28). С. 179-189. URL: https://doi.org/10.52058/2786-5274-2023-14(28)-179-189.

3. Угода між Україною та Європейським Союзом щодо статусу Консультативної місії Європейського Союзу з реформування сектору цивільної безпеки України (КМЄС в Україні) : Угода Україна від 17.11.2014 : станом на 4 лют. 2015 р. URL: https://zakon.rada.gov.ua/laws/show/984_012#Text.

УДК 341.32:336.7

Седляківська К.Г., асистентка кафедри права та правоохоронної діяльності
Державний університет «Житомирська політехніка», м. Житомир

НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО ЗАРУБІЖНИХ КРАЇН У СФЕРІ ПРОТИДІЇ ФІНАНСУВАННЯ ЗБРОЙНИХ КОНФЛІКТІВ

У сучасних умовах глобальної нестабільності та зростання збройних конфліктів питання протидії їх фінансуванню набуває особливої уваги. Збройне вторгнення російської федерації на територію України, яке розпочалося у 2014 році з анексії Криму та набуло повномасштабного характеру у лютому 2022 року, стало яскравим прикладом того, як фінансування збройного конфлікту може відбуватися через як відкриті державні канали, так і приховані фінансові механізми. Відповіддю світової спільноти стало масштабне застосування фінансових санкцій, обмеження доступу до міжнародних ринків капіталу, заморожування активів і блокування банківських рахунків. У цьому контексті особливої актуальності набуло вивчення законодавства зарубіжних країн світу та міжнародних організацій щодо протидії таким формам фінансування. Саме тому пропонуємо проаналізувати законодавство міжнародних організацій та окремих країн.

Першим пропонуємо розглянути відповідь Європейського Союзу на російську агресію проти України. ЄС активізував всі можливі юридичні, економічні та фінансові механізми для протидії як самій війні, так і її фінансуванню. Система європейського права виявилася гнучкою, дієвою та орієнтованою на забезпечення міжнародного правопорядку.

Основу правового інструментарію ЄС у цій сфері становлять нормативно-правові акти щодо боротьби з відмиванням коштів і фінансуванням тероризму. Директива ЄС 2015/849 (так звана Четверта директива AML) запровадила принципи фінансової прозорості, контролю за бенефіціарними власниками та обов'язок звітності для фінансових установ [1]. Згодом Директива ЄС 2018/843 (П'ята директива AML) доповнила попередню, зокрема, регулюванням діяльності, пов'язаної з віртуальними активами [2]. У 2024 році ЄС ухвалив новий регламент ЄС 2024/1624, який встановлює єдині правила боротьби з фінансуванням тероризму, та створив орган AMLA (Anti-Money Laundering Authority), який координуватиме дії країн-членів [3].

Також Європейський Союз запровадив безпрецендентну за масштабом санкційну політику. Було заборонено доступ російських банків до SWIFT, заморожено активи фізичних і юридичних осіб, пов'язаних із військово-промисловим комплексом рф, та обмежено експорт технологій подвійного призначення [4]. У 2025 році ЄС ухвалив 17-й пакет санкцій, спрямований на «тіньовий флот», компанії, що обходять обмеження, та енергетичний сектор [5]. Також готується 18-й пакет санкцій, що включає блокування обхідних механізмів, як-от інфраструктура Nord Stream і нові обмеження на російську нафту [6].

Санкційна політика ЄС координується з США та міжнародними партнерами. Така співпраця дозволяє виявляти нові фінансові загрози та блокувати канали фінансування збройних конфліктів. ЄС також взаємодіє з FATF та іншими організаціями для гармонізації законодавства з глобальними стандартами [7].

Отже, приклад ЄС показує, що різноманітні правові механізми можуть ефективно протидіяти фінансуванню збройних конфліктів. Гнучкість законодавства, інституційна координація та міжнародна солідарність – ключові чинники у цій боротьбі. В умовах нових геополітичних викликів досвід ЄС є цінним зразком правової реакції на загрозу миру.

США. Сполучені Штати Америки мають розгалужену систему правових механізмів для боротьби з фінансуванням збройних конфліктів та тероризму. Центральне місце займає Закон про банківську таємницю (BSA), що зобов'язує фінансові установи повідомляти про великі або підозрілі транзакції [8]. Після подій 11 вересня 2001 року було прийнято Закон USA PATRIOT, який значно розширив можливості уряду з протидії фінансовим потокам, пов'язаним із терористичною діяльність [9]. Ключову роль у реалізації антикризової фінансової політики відіграє FinCEN – Управління з фінансових злочинів Мінфіну США, яке адмініструє BSA і координує зусилля державних структур у сфері фінансової безпеки [10]. Також у 2021 році було ухвалено Закон про корпоративну прозорість (CTA), що зобов'язує компанії розкривати дані про бенефіціарів - це спрямовано на боротьбу з використанням фіктивних компаній для фінансування конфліктів [11]. Окремим інструментом виступає санкційна політика. Наприклад, у 2025 році США наклали санкції на осіб і компанії, пов'язані з мексиканським картелем Сіналоа, за участь у фінансуванні терористичних структур [12].

Велика Британія протидіє фінансуванню збройних конфліктів через законодавство та санкційні механізми. Основою є Закон про санкції та боротьбу з відмиванням грошей 2018 року (SAMLA), який дозволяє уряду вводити санкції проти осіб і організацій, що загрожують міжнародному миру [13]. Також Британія у відповідь на вторгнення росії в Україну заморозила активи понад 1500 пов'язаних осіб [14] та запровадили торговельні обмеження, зокрема на «брудне золото» [15]. У 2025 році країна вперше застосувала санкції до ультраправої групи «Blood and Honour» (неонацистська музична промо-мережа та право радикальна політична група у Великій Британії) за фінансування екстремізму [16]. Також Велика Британія забезпечує виконання міжнародних стандартів FATF, про що свідчить звіт уряду щодо ефективності нагляду у 2023-2024 роках [17].

В свою чергу Україна має комплексне законодавство для протидії фінансування збройних конфліктів, ключовим елементом якого є ЗУ «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», що регулює виявлення, моніторинг та блокування підозрілих фінансових операцій, пов'язаних із терористичною діяльністю [18]. У 2023 році до цього закону були внесені зміни, які посилили вимоги до фінансового моніторингу та розширили перелік суб'єктів, зобов'язаних здійснювати такі заходи. Ці зміни спрямовані на підвищення ефективності виявлення та запобігання фінансування терористичної діяльності та збройних конфліктів [19]. Крім того, Україна активно співпрацює з міжнародними організаціями, такими як FATF, для імплементації міжнародних стандартів у національне законодавство та забезпечення ефективної протидії фінансуванню тероризму на глобальному рівні.

Таким чином, аналіз законодавства провідних міжнародних суб'єктів – ЄС, США, Великої Британії та України – свідчить про зростання ролі правових механізмів у протидії фінансуванню збройних конфліктів. Всі досліджені країни постійно удосконалюють власну нормативну базу у відповідь на нові загрози, що підтверджує важливість комплексного та скоординованого підходу до запобігання ескалації насильства у світі. Україна в цьому контексті не лише приймає відповідні закони, а й демонструє активну участь у формуванні глобального правового поля безпеки.

Список використаних джерел:

1. Counter-Terrorism Module 5 Key Issues: European Region. *United Nations Office on Drugs and Crime*. URL: https://www.unodc.org/e4j/en/terrorism/module-5/key-issues/european-region.html .
2. Anti-money laundering and countering the financing of terrorism at EU level. *Finance*. URL: https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en.
3. The new EU AML/CFT regime has arrived – are you ready?. *Norton Rose Fulbright | Germany | Global law firm*. URL: https://www.nortonrosefulbright.com/en/knowledge/publications/644c5392/the-new-eu-amlcft-regime-has-arrived-are-you-ready.
4. EU sanctions against Russia. *European Council Council of the European Union*. URL: https://www.consilium.europa.eu/en/policies/sanctions-against-russia/.
5. Payne J., Irish J. Time to suffocate Russia's economy after 17th EU sanctions package, France say. *Reuters*. URL: https://www.reuters.com/world/europe/time-suffocate-russias-economy-after-17th-eu-sanctions-package-france-says-2025-05-14/.
6. Gray A., Bytyci F. EU readying new sanctions to increase pressure on Russia, von der Leyen says. *Reuters*. URL: https://www.reuters.com/world/europe/eu-readying-new-sanctions-increase-pressure-russia-von-der-leyen-says-2025-05-16/.
7. Anti-money laundering and countering the financing of terrorism at EU level. *Finance*. URL: https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en.
8. Bank Secrecy Act (BSA) | OCC. *OCC.gov*. URL: https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html.
9. USA PATRIOT Act. *FinCEN.gov*. URL: https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act.
10. History of Anti-Money Laundering Laws. *FinCEN.gov*. URL: https://www.fincen.gov/history-anti-money-laundering-laws.
11. Raymond N. US Supreme Court removes hurdle to anti-money laundering law. *Reuters*. URL: https://www.reuters.com/legal/us-supreme-court-allows-anti-money-laundering-law-take-effect-2025-01-23/.
12. US sanctions Sinaloa Cartel associates for alleged money laundering. *AP News*. URL: https://apnews.com/article/sinaloa-cartel-treasury-department-money-laundering-fentanyl-e976f2219e4588281d19d925ced9e306.
13. A comprehensive overview of sanctions in the United Kingdom. *Global Investigations Review*. URL: https://globalinvestigationsreview.com/guide/the-guide-sanctions/fifth-edition/article/comprehensive-overview-of-sanctions-in-the-united-kingdom .
14. Foreign, Commonwealth & Development Office. UK sanctions following Russia's invasion of Ukraine. URL: https://www.gov.uk/government/collections/uk-sanctions-following-russias-invasion-of-ukraine.
15. US, UK take aim at illicit gold trade in sanctions action. *Reuters*. URL: https://www.reuters.com/world/europe/uk-sanctions-illicit-gold-trade-players-bid-cut-russias-war-funding-2024-12-09/.
16. UK imposes asset freeze on 'extreme right wing group' Blood and Honour. *Reuters*. URL: https://www.reuters.com/world/uk/uk-imposes-asset-freeze-extreme-right-wing-group-blood-honour-2025-01-08/.
17. HM Treasury. Anti-money laundering and countering the financing of terrorism: Supervision Report 2023-24. *GOV.UK*. URL: https://www.gov.uk/government/publications/anti-money-laundering-and-countering-the-financing-of-terrorism-supervision-report-2023-24.
18. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 № 361-IX : станом на 9 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text.
19. Про внесення змін до Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення" щодо політично значущих осіб : Закон України від 17.10.2023 № 3419-IX. URL: https://zakon.rada.gov.ua/laws/show/3419-20#Text.

УДК 351

Супрунова І.В., д.н.держ.упр., доцент,
доцент кафедри національної безпеки, публічного управління та адміністрування
Прокопчук М.Л., аспірант
Державний університет «Житомирська політехніка»

КРИПТОВАЛЮТА ЯК ДЖЕРЕЛО ФІНАНСУВАННЯ МІЖНАРОДНИХ ТЕРОРИСТИЧНИХ ОРГАНІЗАЦІЙ

У сучасному світі стрімкий розвиток криптовалют та блокчейн-технологій призвів до формування альтернативної фінансової екосистеми, яка функціонує паралельно з традиційними банківськими установами. Висока ліквідність, транскордонний характер та можливість анонімізації операцій роблять криптовалюти потенційно привабливим інструментом для фінансування протиправної діяльності, зокрема міжнародного тероризму.

Наведемо ключові фактори, що зумовлюють привабливість використання криптовалют для фінансування діяльності терористичних організацій:

Псевдонімність транзакцій. Незважаючи на те, що більшість блокчейн-мереж забезпечують прозорість транзакцій, ідентифікація кінцевих бенефіціарів залишається проблематичною за відсутності прив'язки криптовалютних адрес до персональних даних.

Децентралізований характер. Відсутність єдиного емісійного центру та контролюючого органу ускладнює імплементацію традиційних механізмів фінансового моніторингу.

Транскордонність операцій. Криптовалютні транзакції здійснюються без урахування державних кордонів, що дозволяє обходити міжнародні санкції та ембарго.

Швидкість та низька вартість транзакцій. Сучасні криптовалютні системи забезпечують миттєві глобальні перекази з мінімальними комісіями.

У світових масштабах фінансування терористичної діяльності за допомогою криптовалюти зростає, особливо на тлі використання штучного інтелекту для удосконалення атак. За даними дослідницької компанії Chainalysis [2] в 2024 році близько 20% усіх терактів спонсорувалося саме за допомогою криптовалют.

Отже, для мінімізації ризиків використання цифрових активів для фінансування міжнародного тероризму необхідним є системний підхід до регулювання криптовалютного ринку. Враховуючи міжнародний досвід доцільним є: розробка та імплементація міжнародних стандартів регулювання криптовалютної діяльності; впровадження ризик-орієнтованого підходу до моніторингу криптовалютних транзакцій та створення спеціалізованих підрозділів у структурі правоохоронних органів для протидії використанню криптовалют у терористичних цілях.

Список використаних джерел:

1. The Financial Action Task Force (FATF). URL: https://www.fatf-gafi.org/en/home.html.
2. The 2025 Crypto Crime Report. Chainalysis. URL https://go.chainalysis.com/2025-Crypto-Crime-Report.html

УДК 355/359.07;342.08

Філонов М.В., здобувач вищої освіти
Класичний приватний університет

НАУКОВИЙ ДИСКУРС ЩОДО ПРОБЛЕМ ФОРМУВАННЯ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РЕГІОНАЛЬНОМУ РІВНІ В УМОВАХ ЦИФРОВІЗАЦІЇ

Проти України, від моменту проголошення незалежності, ведеться цілеспрямована інформаційна війна з боку сусідньої держави-агресорки. Як результат, її дії створили необхідне підґрунтя для підтримки з боку певної частини українського населення «ідеї руського миру». На жаль, такий деструкт негативно позначається на всій системі безпеки України, боротися з яким їй доведодиться повсяк час [1]. Складності ситуації додає те, що зниження рівня інформаційної безпеки в Україні – це результат соціальної згоди, неофіційної легітимації. Відтак, важливим завданням для нашої держави є не тільки протистояння інформаційним загрозам рф, а й формування високої культури серед українців патріотизму та об'єктивного сприйняття навколишньої інформації.

У сучасних умовах цифрової трансформації суспільства проблема забезпечення інформаційної безпеки набуває особливого значення. Регіональний рівень управління часто залишається найбільш вразливим через обмежені ресурси, недостатню кадрову спроможність та низьку інтеграцію в загальнодержавні цифрові стратегії. Це створює потребу в науковому аналізі механізмів формування ефективної моделі публічного управління інформаційною безпекою на регіональному рівні.

Отже, цифровізація є одним із найбільш вагомих факторів трансформації системи публічного управління у сфері інформаційної безпеки. Цифровізація трансформує не лише економічні та соціальні процеси, а й принципи державного управління. Використання цифрових платформ, відкритих даних, інтелектуальних систем управління змінює характер взаємодії між громадянами, владою та бізнесом. Проте зростання цифрової активності супроводжується й новими ризиками: кіберзлочинністю, витоками персональних даних, дезінформацією, які потребують системного регулювання на регіональному рівні [1; 2].

Зважаючи на це, можемо виокремити основні проблеми формування публічного управління у сфері інформаційної безпеки України на регіональному рівні, а саме:

1. Фрагментованість нормативно-правової бази у сфері забезпечення інформаційної безпеки регіонів. Відсутність уніфікованої законодавчої політики щодо інформаційної безпеки на регіональному рівні призводить до нерівномірного впровадження стандартів.

2. Недостатня координація між центром і регіонами в питаннях забезпечення інформаційної безпеки. Непоодинокими є випадки, коли відсутні ефективні управлінські механізми передачі повноважень, фінансування і відповідальності у сфері кібербезпеки на місця.

3. Кадровий голод. Брак кваліфікованих ІТ-спеціалістів в органах державної влади та місцевого самоврядування ускладнює реалізацію регіональних стратегій захисту інформації на місцях.

4. Недовіра громадян до цифрових сервісів. Зниження рівня цифрової довіри уповільнює процес впровадження новітніх технологій у публічне адміністрування [1; 2].

Усе вищевказане дає підстави для висловлення гіпотези щодо актуалізації наукового дискурсу з питань удосконалення публічного управління інформаційною безпекою, що (дискурс) охоплює такі підходи:

1. Системний підхід. Інформаційна безпека в державі та регіонах має розглядатися як частина ширшої системи національної безпеки, інтегрованої в цифрову стратегію регіону.

2. Децентралізоване управління. Розширення повноважень органів місцевого самоврядування у питаннях безпеки цифрової інфраструктури – це значний крок уперед у гарантуванні безпечного інфопростору для розвитку регіонів [3].

3. Мережевий підхід. Взаємодія органів влади з громадським сектором, бізнесом, ІТ-компаніями та науковими установами з метою створення спільних рішень у сфері кібербезпеки.

4. Функціональний підхід, що передбачає здійснення оцінки ризиків та кіберстійкість регіонів. Власне, необхідною є розробка регіональних механізмів моніторингу загроз та оперативного реагування на інциденти інформаційного впливу, а також регіональних стратегій інформаційної безпеки.

Очевидно, що гібридна війна рф, що ведеться проти України, актуалізує питання щодо визначення ролі регіональних стратегій у забезпеченні інформаційної безпеки. Регіональні стратегії мають бути орієнтовані на адаптацію до специфіки місцевих викликів. Це вимагає:

– створення локальних центрів кіберзахисту;

– розробки освітніх програм для підвищення цифрової грамотності чиновників та громадян;

– упровадження інструментів е-демократії з високим рівнем захисту персональних даних.

Таким чином, результативне й ефективне публічне управління у сфері інформаційної безпеки на регіональному рівні в Україні потребує переходу до нової управлінської парадигми, в якій мають поєднуватися інноваційність, відкритість та відповідальність. У цьому контексті можемо наголосити на

необхідності посилення наукового забезпечення управлінських рішень, удосконалення законодавчої та підзаконної правової бази, а також розвитку регіональних інституційних і цифрових екосистем як основи для формування безпечного інформаційного простору держави загалом і регіонів зокрема.

Список використаних джерел:

1. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в державному секторі : монографія. 2024. Харків: НУЦЗУ. 244 с. URL: http://repositsc.nuczu.edu.ua/handle/123456789/19990.

2. Новіков В.О. Information and hybrid wars in the current environment: public-administrative aspect // Public administration and state security aspects. 2023. Vol. 2. P. 43–51.

3. Почепцов Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії. Харків : Віват, 2022. 384 с.