МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
КИЇВСЬКИЙ ІНСТИТУТ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ
ФАКУЛЬТЕТ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ
КАФЕДРА ДЕРЖАВНОЇ БЕЗПЕКИ

«МАГІСТЕРСЬКА РОБОТА ЗА ФАХОМ»

тема

ОЦІНКА РИЗИКІВ ТЕРОРИЗМУ В УКРАЇНІ

здобувача вищої освіти
другого (магістерського) рівня
вищої освіти освітньо-професійної
програми 251 «Державна безпека»
Спеціалізація – Організація
забезпечення державної безпеки
підрозділами Національної гвардії
України
Гриценко Сергія
Володимировича
Науковий керівник:
Павлов Дмитрій Вадимович
Професор кафедри державної
безпеки.
Кандидат військових наук. Старший
науковий співробітник

Магістерська робота захищена
з оцінкою_____
«___»_____20__р.

Київ - 2025

ABSTRACT

Hrytsenko Serhii Volodymyrovych

«Terrorism Risk Assessment in Ukraine». – Manuscript.

Master's Thesis in Specialty 251 "State Security" – Kyiv Institute of the National Guard of Ukraine, Kyiv, 2024.

The master's thesis is devoted to a comprehensive study of the problem of terrorism risk assessment in Ukraine in the context of hybrid aggression and the transformation of the national security environment. It is determined that effective assessment of terrorist risks is a crucial prerequisite for the development of state counterterrorism policy and for ensuring the resilience of state institutions to destructive influences.

The thesis outlines the theoretical foundations of the concept of terrorism, its legal and interdisciplinary characteristics, the classification of threats, as well as modern approaches to terrorism risk analysis. The dynamics of terrorist threats in Ukraine during 2014–2024 are analyzed, and the main shortcomings of the existing response system are identified. Particular attention is paid to the technological aspects of improving risk assessment tools, including the application of analytical platforms, artificial intelligence algorithms, and interagency information exchange mechanisms.

The author proposes a model for enhancing the national terrorism risk assessment system, taking into account international experience, and develops a conceptual framework for the transition to a preventive and predictive model of risk governance in the counterterrorism sphere.

Keywords: terrorism, risk assessment, national security, hybrid warfare, security analytics, interagency cooperation, information threat, predictive systems, prevention.

ВСТУП

Актуальність теми зумовлена трансформацією характеру терористичних загроз в умовах гібридної війни та радикальним ускладненням безпекового середовища внаслідок динамічного розвитку новітніх форм тероризму — кібертерору, інформаційно-психологічних впливів, автономної радикалізації,

використання цивільної інфраструктури як об’єкта атак. Упродовж 2014–2024 років Україна стала полем постійного терористичного тиску, що супроводжується як прямими насильницькими актами, так і прихованими формами організованого впливу, зокрема через диверсійно-розвідувальні мережі, маніпулятивні наративи, сплячі осередки та фінансову підтримку деструктивних угруповань.

Проблемність теми полягає у відсутності системної, інтегрованої та прогностичної моделі оцінки ризиків тероризму в Україні, яка могла б ефективно поєднувати міжвідомчу інформацію, сучасні аналітичні інструменти, нормативну визначеність і стратегії реагування. Діючі підходи залишаються фрагментарними, переважно реактивними, орієнтованими на постфактум-фіксацію загроз, що не відповідає викликам терористичних технологій нового типу — зокрема, автономізованого терору без централізованого управління або масового терору в інформаційному середовищі. Це, у свою чергу, обумовлює зростаючий дефіцит аналітичної передбачуваності, обґрунтованої профілактики і науково-технологічної готовності державної системи безпеки до нових викликів.

Теоретична значущість теми полягає в необхідності глибшого осмислення сутності тероризму як багатовимірного соціально-правового явища, що вимагає міждисциплінарного підходу для його розуміння: поєднання кримінально-правової доктрини, безпекознавчих концепцій, аналітичної кібернетики, соціальної психології та політології. Практична важливість дослідження зумовлена потребою в удосконаленні національного механізму оцінки ризиків, що має стати інструментом випереджувальної антитерористичної політики — орієнтованої на виявлення, нейтралізацію та запобігання загрозам ще до моменту їхньої реалізації.

Таким чином, актуальність теми зумовлена не лише зростанням терористичних ризиків, а й наявністю низки концептуальних і прикладних проблем, які не дозволяють ефективно реагувати на них у сучасних умовах. Вивчення цих проблем та пошук шляхів їхнього вирішення становить необхідну передумову для підвищення стійкості національної безпеки України.

Аналіз останніх досліджень і публікацій. Проблематика тероризму, його правової кваліфікації, соціально-політичної природи та механізмів запобігання протягом останніх років активно досліджується як у вітчизняній, так і в зарубіжній науковій думці.

У вітчизняній науковій літературі сутнісні характеристики тероризму як кримінального явища розглядаються у працях таких правознавців, як В.Я. Тацій, О.М. Литвинов, М.І. Бажанов, які аналізують терористичні злочини у контексті кримінального права, питання кваліфікації терористичних актів, а також розмежування тероризму з іншими суміжними злочинами — диверсією, масовими заворушеннями, посяганнями на державну владу. У роботах І.О. Коляди, Ю.І. Римаренка, В.П. Шепети піднімаються питання соціальної природи тероризму, радикалізації та впливу інформаційного простору на процеси вербування до терористичних структур. Окрему увагу приділено міждисциплінарному аналізу тероризму як політичного феномену, що набуває нових форм у межах гібридних конфліктів.

Суттєвий внесок у вивчення проблем національної безпеки й системи боротьби з терористичними загрозами зроблено С.В. Чернявським, який досліджує питання організаційно-правового механізму антитерористичної політики України, та О.В. Яковлєвою, яка акцентує увагу на необхідності інтеграції превентивних підходів у роботу правоохоронних органів.

Об’єкт дослідження. Механізми функціонування системи національної безпеки України в умовах терористичних загроз, а також управлінські, правові та організаційні процеси, пов’язані з ідентифікацією, оцінкою та запобіганням терористичній активності.

Предмет дослідження. Теоретичні засади, правові конструкції та практичні інструменти оцінки ризиків терористичних загроз в Україні, їхня ефективність, взаємодія між суб’єктами протидії тероризму, а також можливості удосконалення моделей ризик-аналізу в умовах гібридної безпеки.

Мета дослідження. Комплексно проаналізувати сучасний стан і проблематику оцінки терористичних ризиків в Україні, виявити системні вразливості та розробити науково обґрунтовані підходи до вдосконалення

національної моделі аналізу й управління ризиками у сфері протидії тероризму з урахуванням актуальних викликів безпекового середовища.

Відповідно до мети дослідження окреслено наступні завдання:

1. Розкрити змістовну сутність тероризму як суспільно небезпечного явища та здійснити класифікацію основних типів терористичних загроз за критеріями їх походження, форм реалізації та спрямованості.
2. Дослідити сучасні наукові підходи до визначення терористичних ризиків та проаналізувати основні методи їх оцінки, що застосовуються у практиці протидії тероризму на національному та міжнародному рівнях.
3. Здійснити аналіз динаміки та специфіки розвитку терористичних загроз в Україні у період з 2014 по 2024 роки, з урахуванням гібридного характеру сучасної війни та новітніх форм деструктивної діяльності.
4. Визначити ключові проблеми, слабкі місця та системні недоліки у чинній моделі оцінки терористичних ризиків, що функціонує в українській безпековій системі.
5. Обґрунтувати науково-практичні напрями вдосконалення системи оцінки ризиків тероризму в Україні, включаючи пропозиції щодо правового, організаційного та аналітичного оновлення, з урахуванням світових стандартів і технологічного прогресу.

У процесі дослідження використано комплекс загальнонаукових, спеціально-юридичних та міждисциплінарних **методів**. Метод логіко-структурного аналізу застосовано при класифікації терористичних загроз і виокремленні їхніх ключових ознак, метод системного підходу використовувався для оцінки взаємозв’язків між суб’єктами протидії тероризму та аналізу їхньої ролі у формуванні єдиної системи оцінки ризиків, порівняльно-правовий метод використано для зіставлення вітчизняних підходів до оцінювання терористичних загроз з міжнародними практиками, методи індукції та дедукції застосовувалися під час формування авторських висновків щодо необхідності модернізації інституційного та технологічного інструментарію національної системи безпеки.

Наукова новизна отриманих результатів. У межах дослідження удосконалено понятійно-категоріальний апарат, що використовується для аналізу терористичних загроз, зокрема запропоновано авторське розмежування понять «терористичний ризик» та «терористична загроза» як окремих етапів і форм у ланцюгу деструктивної активності. Одержав подальший розвиток підхід до розгляду оцінки ризиків тероризму як динамічного процесу, що вимагає поєднання правових, аналітичних і технологічних компонентів. Конкретизовано особливості функціонування системи оцінки ризиків тероризму в умовах гібридної агресії. Запропоновано авторську модель напрямів вдосконалення цієї системи, що включає впровадження міжвідомчої платформи аналітичного обміну, використання інструментів штучного інтелекту для аналізу даних та формування національної карти ризиків. Визначено концептуальні засади переходу від реактивної до превентивно-аналітичної моделі управління терористичними загрозами в Україні.

Структура магістерської роботи побудована відповідно до логіки дослідження та визначених завдань. У першому розділі викладено теоретико-методологічні основи оцінки ризиків тероризму, розкрито зміст та класифікацію терористичних загроз, а також проаналізовано сучасні методи їх ідентифікації й аналізу. Другий розділ присвячено аналізу сучасного стану терористичних загроз в Україні та обґрунтуванню науково-практичних напрямів вдосконалення національної системи оцінки ризиків. Обсяг роботи становить 70 сторінок основного тексту (без урахування списку використаних джерел), у ній використано 44 джерела, серед яких нормативно-правові акти, наукові праці вітчизняних і зарубіжних авторів, аналітичні звіти, міжнародні документи та публікації спеціалізованих організацій у сфері безпеки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ОЦІНКИ РИЗИКІВ ТЕРОРИЗМУ

1.1. Поняття та класифікація терористичних загроз

У контексті глобалізованого світу XXI століття тероризм набув ознак багатогранного, складного соціально-політичного феномену, який безпосередньо впливає на безпекову архітектоніку як на національному, так і на міжнародному рівнях. Його динамічний характер, транснаціональні прояви та здатність до адаптації під сучасні технологічні умови створюють необхідність поглибленого наукового аналізу понять, форм, методів та класифікаційних ознак терористичних загроз, що становлять собою ключовий елемент у процесі системної оцінки ризиків тероризму. Розкриття теоретичних засад цього явища є критичним для формування ефективних державних політик у сфері протидії тероризму та розробки стратегій зниження його потенційного впливу [25].

Поняття терористичної загрози, як об'єкта наукового дослідження, має складну структурну природу, що поєднує елементи кримінального, політичного, соціального та навіть психологічного аналізу. У загальноприйнятому академічному розумінні, терористична загроза — це сукупність реальних або потенційних умов, чинників та дій, що спрямовані на дестабілізацію суспільно-політичного устрою, порушення громадської безпеки, залякування населення чи уряду через застосування або погрозу застосування насильства, зокрема з використанням вибухових речовин, зброї, кіберзасобів тощо [17]. Під цим терміном розуміється не лише безпосередній акт насильства, але і вся система факторів, що можуть зумовити його реалізацію або сприяти її ймовірності.

Семантично термін «тероризм» походить від латинського *terror* — страх, жах, що вже на етимологічному рівні свідчить про сутнісну характеристику терористичної діяльності: створення атмосфери страху для досягнення певних цілей [16]. З точки зору національного законодавства, а також у контексті міжнародних нормативно-правових актів (зокрема, резолюцій Ради Безпеки ООН, рекомендацій FATF, документів ЄС та НАТО), терористичні загрози поділяються на внутрішні та зовнішні, актуальні та потенційні, організовані та

спорадичні, симетричні та асиметричні. Кожна з цих класифікацій має не лише теоретичне, але й практичне значення для ідентифікації загроз, їх моделювання та прогнозування.

Поглиблене осмислення юридичного змісту поняття «тероризм» неможливе без системного аналізу відповідного законодавства, а також критичної оцінки наявних дефініцій з позицій кримінально-правової, кримінологічної та міждисциплінарної методології. У цьому контексті особливої уваги заслуговує Закон України «Про боротьбу з тероризмом» 2003 року, в якому тероризм трактується як суспільно небезпечна діяльність, що полягає у свідомому, цілеспрямованому застосуванні насильства — через захоплення заручників, вбивства, підпали, тортури, інші посягання на життя і здоров'я людей, або в погрозі вчинення таких дій задля досягнення певних злочинних цілей [23]. Попри значення цієї законодавчої дефініції як базисної для системи протидії тероризму в Україні, вона не може бути визнана зразком кримінально-правової категорії у вузькому сенсі, оскільки має надто загальний, дескриптивний характер і радше функціонує в кримінологічному чи соціологічному полі.

Ключовий недолік вищенаведеного визначення полягає у відсутності чіткої нормативної прив'язки між самим актом насильства та його метою, що є визначальним критерієм у кримінальному праві. Злочин не може бути кваліфікований без урахування суб'єктивної сторони, зокрема мотиву й цілі діяння. Цей аспект чітко розкривається у диспозиції статті 258 Кримінального кодексу України, в якій терористичний акт визначається як суспільно небезпечне діяння, спрямоване на вплив на прийняття рішень або дій державними органами, органами місцевого самоврядування, юридичними особами чи об'єднаннями громадян, а також задля привернення уваги до певних поглядів винного. Тобто юридична кваліфікація терористичного злочину передбачає не лише факт застосування насильства або його погрози, а й наявність стратегічного «меседжу» — цілеспрямованої комунікації з владними структурами та суспільством, яка і є визначальною ознакою тероризму як окремого типу кримінального делікту.

В юридичному плані тероризм можна розглядати як складний правовий феномен, що охоплює кілька рівнів — кримінально-правовий, адміністративно-правовий, міжнародно-правовий, а також інституційний рівень державної політики безпеки [19]. На кримінально-правовому рівні важливим є виокремлення чітких ознак складу злочину: об’єкт (громадська безпека, функціонування органів влади), об’єктивна сторона (насильство або погроза його застосування), суб’єкт (фізична осудна особа), суб’єктивна сторона (прямий умисел із політичною, ідеологічною або релігійною метою). Саме наявність спеціальної мети, що виходить за межі звичайної мотивації у кримінальному праві, створює додану складність в оцінці терористичних загроз.

Важливо зазначити, що з погляду правової доктрини тероризм має три взаємопов’язані характеристики: перше — це факт насильницького діяння або його реальної загрози; друге — спрямованість проти невизначеного кола осіб або об'єктів, що є ознакою терору як публічного явища; третє — наявність ідеологічно або політично вмотивованої цілі [19]. Ці елементи є ключовими для розмежування тероризму від інших злочинів насильницького характеру, таких як убивства з корисливих мотивів або хуліганство з особливою жорстокістю. Тероризм, у цьому сенсі, є злочином комунікативного типу: його ефективність вимірюється не лише кількістю жертв чи обсягом завданих збитків, а насамперед здатністю породити страх, нестабільність, вплинути на масову свідомість і ухвалення політичних рішень.

Загалом, юридичний зміст тероризму — це багатовимірне, багатофакторне і динамічне поняття, що охоплює не лише формальні ознаки складу злочину, а й функціонує в ширшому контексті політико-правової взаємодії держави і суспільства. Його розуміння вимагає поєднання нормативного аналізу з доктринальним осмисленням, з урахуванням сучасних тенденцій безпекового середовища, включно з цифровізацією, міжнародною координацією боротьби з тероризмом і розширенням спектру форм, методів та інструментів терористичної діяльності. Це робить юридичну категорію «тероризм» не лише правовим терміном, а й концептом, що відображає складні трансформаційні процеси у сфері безпеки, справедливості й публічного управління.

Законодавче визначення терористичного акту, закріплене в диспозиції статті 258 Кримінального кодексу України, на перший погляд, є доволі розгорнутим і структурно впорядкованим. Воно охоплює як форми прояву терористичного насильства, так і цілі, які стоять за вчиненням відповідних діянь. Однак правовий аналіз свідчить, що незважаючи на уявну завершеність дефініції, вона залишає відкритими низку важливих аспектів, які безпосередньо впливають на правозастосування, зокрема ідентифікацію терористичного акту серед суміжних за формою або наслідками кримінальних деліктів.

Терористичний акт у розумінні ст. 258 КК України передбачає наявність таких складових: застосування зброї, вибуху, підпалу чи інших дій, які створюють небезпеку для життя чи здоров'я людей, або спричиняють значну майнову шкоду чи інші тяжкі наслідки [13]. Однак головною, визначальною ознакою цього злочину виступає не форма, а ціль діяння: порушення громадської безпеки, залякування населення, провокація воєнного конфлікту, вплив на рішення органів влади або привернення уваги до певних ідеологічних позицій винного. У такий спосіб законодавство підкреслює, що не кожне суспільно небезпечне застосування насильства кваліфікується як терористичний акт — визначальним є суб'єктивний елемент, що надає діянню характеру політично, релігійно або ідеологічно вмотивованої публічної агресії.

Однією з головних проблем, яка супроводжує визначення терористичного акту, є відмежування його від інших злочинів, які зовні можуть бути тотожними за способом вчинення — наприклад, від масових заворушень, умисного вбивства, знищення майна, диверсії або саботажу. У цьому контексті науковець О.В. Хаваліц цілком слушно зауважує, що на сьогодні існує близько 200 різних дефініцій тероризму, запропонованих у науковій літературі, які суттєво різняться між собою за ознаками суб'єкта, мети, мотивації та форм дії [38]. Ця множинність підходів свідчить про відсутність єдності в розумінні сутності терористичного явища як на доктринальному, так і на нормативному рівнях. Причина полягає не лише у нечіткості юридичних формулювань, а передусім у мінливості й адаптивності самого феномену тероризму, його здатності до

трансформації відповідно до нових технологій, політичних умов, соціального контексту.

Слід зазначити, що в українській правовій доктрині сформувалась ціла низка підходів до тлумачення терористичного акту як кримінально-караного діяння. Зокрема, дослідниця О.С. Попович у своєму дисертаційному дослідженні пропонує більш структуровану дефініцію, яка має на меті конкретизацію загальнонебезпечного характеру дій, розширення кола об'єктів впливу та виокремлення цільових установок як критерію кваліфікації [23]. Вона пропонує визначати терористичний акт як застосування зброї, вчинення вибуху, підпалу або іншого загальнонебезпечного діяння, що спрямоване на залякування населення або окремої соціальної групи, створює небезпеку для життя або здоров'я людей, заподіює значну майнову шкоду або інші тяжкі наслідки, вчинене з метою дестабілізації діяльності державних інституцій, органів місцевого самоврядування або громадських об'єднань [23].

Крім того, заслуговує уваги й редакційна пропозиція В.П. Ємельянова, який, відштовхуючись від реалістичного криміналістичного аналізу, пропонує дещо лаконічнішу, але структурно вивірену редакцію диспозиції. Згідно з нею, терористичний акт – це вчинення або погроза вчинення вибуху, підпалу чи інших загальнонебезпечних дій, спрямованих на залякування населення з метою впливу на прийняття рішень державними, місцевими чи міжнародними органами або окремими суб'єктами [6]. Така редакція формує більш чітке співвідношення між способом діяння і його цільовою орієнтацією, виводячи на перший план не тільки факт небезпеки, але й інституціональний вектор терористичного впливу.

Незважаючи на це, обидві авторські моделі демонструють спільний тренд у напрямку відмови від універсалізму на користь точнішої юридичної мови та структурного членування ознак складу злочину. Цей підхід є відповіддю на загальнотеоретичну проблему багатозначності поняття «тероризм» у сучасній правовій науці. Адже, як слушно зазначає дослідниця О.В. Хаваліц, на сьогодні у наукових джерелах циркулює понад 200 різних дефініцій поняття «тероризм», і жодна з них не має універсального визнання. Причина полягає не лише у варіативності форм прояву терористичних дій, але й у складності юридичної

категоризації мотивів, суб'єктів і об'єктів таких діянь, що постійно модифікуються під впливом соціально-політичної кон'юнктури.

Ситуація ускладнюється ще й тим, що на рівні міжнародного права також немає єдиного підходу до дефініції тероризму. Конвенційна база, починаючи від Міжнародної конвенції про боротьбу з бомбовим тероризмом (1997 р.) і закінчуючи резолюціями Ради Безпеки ООН, містить лише фрагментарні ознаки цього явища. Відповідно, національні правові системи змушені виробляти власні підходи до криміналізації терористичних дій, нерідко із залученням елементів внутрішньополітичної риторики, що негативно впливає на об'єктивність кваліфікації та правову визначеність.

У цьому контексті правозастосовна практика вимагає більш точного юридичного інструментарію, який дозволить однозначно визначити склад злочину, відмежувати його від суміжних деліктів і забезпечити передбачуваність судових рішень. Наявна дефініція в ст. 258 КК України, навіть з урахуванням тлумачень судової практики та наукових коментарів, не виконує цієї функції в повній мірі [13]. З огляду на викладене, необхідним є проведення кодифікаційної роботи щодо уточнення не лише поняття «терористичний акт», але й суміжних термінів – «тероризм», «терористична діяльність», «терористична організація». Ця робота має базуватись на міждисциплінарному підході, який поєднує кримінальне право, кримінологію, політологію, соціологію, міжнародне право та інформаційні технології (в умовах зростання кібертероризму).

Питання дефініювання терористичного акту у кримінальному праві України продовжує залишатися однією з ключових та водночас дискусійних площин сучасної юридичної науки. Аналізуючи як чинне законодавче визначення, так і наукові підходи до його тлумачення, виявляється глибинна проблема змістовного розриву між формально-правовими ознаками і фактичними проявами терористичних дій у соціальній реальності [6]. Актуальність цієї теми зумовлена як інтенсивністю розвитку глобальних загроз терористичного характеру, так і об'єктивною необхідністю правової уніфікації та ясності у визначенні понять, які мають стратегічне значення для національної безпеки.

Законодавче закріплення термінів, пов'язаних із терористичною діяльністю, реалізоване в Україні у кількох нормативно-правових джерелах, ключовим серед яких є Кримінальний кодекс України та Закон України «Про боротьбу з тероризмом» [24]. Так, згідно з чинною редакцією ст. 258 КК України, терористичний акт визначається як використання зброї, вчинення вибуху, підпалу чи інших дій, що створюють небезпеку для життя чи здоров'я людей, значні майнові втрати або інші тяжкі наслідки, якщо вони вчиняються з метою порушення громадської безпеки, залякування населення чи впливу на рішення органів державної влади або місцевого самоврядування, а також міжнародних організацій [13]. Це визначення є базовим, однак уже тривалий час зазнає критики з боку науковців за надмірну загальність і відсутність чітко структурованих юридичних ознак, необхідних для стабільного та об'єктивного правозастосування.

Наукове осмислення зазначеної дефініції дозволяє виділити два ключові підходи до її аналізу. Перший — це так званий «розширений» підхід, який орієнтований на включення до терористичних актів якнайширшого кола суспільно небезпечних дій. Саме цього підходу дотримується О.С. Попович, яка у своєму дисертаційному дослідженні пропонує авторське визначення, у якому робить акцент на наслідках вчиненого діяння (створення небезпеки для життя, майнової шкоди, інших тяжких наслідків), мотивації (залякування соціальної групи) та кінцевій меті (дестабілізація органів влади, вплив на їхнє рішення) [23]. Ця дефініція вирізняється більш гнучкою побудовою і намагається систематизувати поняття шляхом деталізації об'єктивної та суб'єктивної сторін злочину. Проте, критичним моментом залишається відсутність онтологічної відмінності між терористичним актом і низкою інших загальнонебезпечних злочинів (наприклад, диверсією, захопленням заручників, умисним знищенням майна), що ускладнює кваліфікацію діяння у реальній правозастосовній практиці.

Іншим підходом є нормативізація концепції терористичного акту через переосмислення самого феномену тероризму як політичного та кримінально-правового явища. Цього напрямку дотримується, зокрема, В.П. Ємельянов, який

наполягає на деполітизації тероризму. Він підкреслює, що відхід від політичного тлумачення є необхідним як з огляду на точність правозастосування, так і з метою недопущення використання антитерористичних законів для репресій чи придушення політичної опозиції [6]. На його думку, тероризм повинен кваліфікуватися виключно за критеріями загальної суспільної небезпеки, публічності дій і наявності впливу на психоемоційну атмосферу у суспільстві. У його запропонованій редакції ст. 258 КК України чітко проглядається спроба сконцентрувати увагу на меті дій (вплив на рішення, залякування), а також включити до переліку таких форм як отруєння, затоплення, викрадення осіб, посягання на радіоактивні матеріали, що формує більш комплексне та багатогранне визначення [13].

Особливої уваги потребує критичний аналіз законодавчого визначення тероризму, яке надано у ст. 1 Закону України «Про боротьбу з тероризмом» [24]. У цьому визначенні фокусується увага на насильницькому характері дій, їхній спрямованості проти невинних осіб і використанні таких засобів як захоплення заручників, тортури, убивства тощо. При цьому головна мета — досягнення злочинних цілей через психологічний вплив, тобто навіювання страху. Попри начебто достатню змістовну наповненість, ця дефініція є більш декларативною, ніж операційною, оскільки відсутні чіткі критерії для юридичної оцінки конкретного діяння як терористичного, зокрема не визначено межу між терористичним актом і звичайним убивством, захопленням заручників чи диверсією, вчиненою без ідеологічного або політичного підґрунтя.

Особливе значення у проблематиці дефініювання терористичного акту має питання відмежування його від суміжних складів злочинів. Існує низка кримінально-правових деліктів, які можуть за формою бути ідентичними терористичному акту — наприклад, вибухи, вбивства, викрадення — однак не мають терористичної мети, а отже, не повинні підпадати під дію ст. 258 КК України. Проте недосконалість законодавчої техніки та розмитість визначення терористичного акту призводять до того, що межі між цими злочинами залишаються умовними, а правозастосовна практика не має єдиної позиції з приводу їх кваліфікації [26]. Це є серйозним викликом не лише для органів

досудового розслідування, а й для судів, які змушені інтерпретувати норми за відсутності чіткого законодавчого орієнтиру.

Отже, нагальною залишається потреба в розробці уніфікованого, теоретично виваженого й юридично точного визначення понять «терористичний акт», «тероризм», «терористична організація», яке б спиралося як на правову доктрину, так і на емпіричні дані з правозастосовної практики. Таке визначення повинно враховувати специфіку суб'єкта, форму вини, мету, спосіб вчинення діяння, його наслідки, а також суспільний резонанс. Лише тоді буде можливим створення стабільної, передбачуваної та об'єктивної системи боротьби з терористичними проявами, що є необхідною передумовою захисту демократичного ладу та національної безпеки України [31].

Тероризм як соціально-правове явище набуває особливого значення в умовах глобальних загроз сучасності, спричинених як внутрішніми, так і зовнішніми чинниками політичної, релігійної, ідеологічної чи соціальної дестабілізації. Особливого теоретико-прикладного інтересу набуває визначення й осмислення терористичного акту як конкретної форми реалізації терористичної ідеології у вигляді суспільно небезпечного злочинного діяння. З погляду кримінального права, терористичний акт виступає формалізованим проявом загального явища тероризму, набуваючи конкретного змісту лише в процесі здійснення одиничного акту насильства з чітко визначеною метою і способом впливу на суспільно-політичні процеси.

Л. М. Демидова та О. С. Попович у своїх наукових працях слушно вказують, що терористичний акт становить собою окремий різновид терористичної діяльності, що характеризується специфічними рисами, зокрема: наявністю загальної небезпеки, публічністю вчинення, а також спрямованістю на досягнення конкретної або загальної мети [5]. Ці автори вказують на органічний зв'язок між поняттями «тероризм» і «терористичний акт», що обумовлює неможливість їх розмежування без урахування діалектичного співвідношення загального й одиничного. У цьому аспекті заслуговує на увагу застосування матеріалістичної діалектики як методологічного підходу, відповідно до якого тероризм розглядається як загальне явище, що містить у собі потенційно

необмежене коло форм прояву, в той час як терористичний акт — це одинична, конкретна реалізація цього явища, яка надає тероризму фактичного втілення через певний набір дій, що мають кримінально-караний характер [5].

Значущою характеристикою терористичного акту є його публічність і демонстративність. Це пояснюється тим, що цільовою аудиторією дій терориста є не лише безпосередні жертви злочину, а набагато ширше коло соціальних суб'єктів, у тому числі органи влади, міжнародна спільнота, громадськість, медіа. Цим самим підкреслюється специфічна соціальна природа терористичних діянь, які, хоч і вчиняються індивідом чи групою осіб, за своїм значенням носять надперсональний характер. Відтак терористичний акт є комунікативним актом, через який винний суб'єкт адресує власне послання суспільству або конкретній цільовій групі, використовуючи насильство як мовну категорію [9]. В контексті теорії соціальної комунікації, терористичний акт виконує роль маркера конфлікту, який привертає увагу до певної проблематики або вимагає зміни політичного статусу-кво.

У сучасному правозастосовному полі важливим є розуміння погрози вчинення терористичного акту як самостійного виду терористичного злочину. У чинній редакції ст. 258 КК України вказано, що навіть погроза вчинення відповідних дій (вибуху, підпалу, застосування зброї тощо) з означеною вище метою є підставою для притягнення до кримінальної відповідальності. Це положення законодавець формулює, виходячи з превентивної функції кримінального права: суспільство має бути захищеним не лише від реалізованих форм терористичної агресії, а й від загрози її здійснення. Такий підхід відповідає доктрині загальносоціального попередження злочинів, яка передбачає завчасне реагування на загрозливі сигнали, що виходять із соціального середовища.

Особливої уваги заслуговує зв'язок терористичного акту з глобальними процесами трансформації злочинності, зокрема інтернаціоналізацією кримінальних загроз та гібридизацією форм насильства. Сучасний тероризм дедалі частіше набуває транскордонного характеру, що ускладнює ідентифікацію виконавців, координацію міждержавної протидії, а також уніфікацію правових підходів до класифікації діянь. У цьому контексті

терористичний акт виступає як точка перетину кримінального, політичного та міжнародного виміру, набуваючи ускладненого характеру, що потребує мультидисциплінарного підходу у дослідженні [2].

З огляду на викладене, стає очевидним, що терористичний акт є надзвичайно складним і багатогранним явищем, яке водночас є юридично значущим злочином, соціальним сигналом та політичним інструментом. Його розуміння вимагає поєднання кримінально-правового, соціологічного, філософського та міжнародно-правового аналізу. У працях вітчизняних правників, зокрема В. П. Ємельянова, Л. М. Демидової та О. С. Попович, запропоновано концептуальні підходи до правового визначення тероризму та терористичного акту, які дозволяють сформулювати цілісну доктрину терористичної відповідальності, засновану на принципах правової визначеності, юридичної точності та соціальної доцільності.

Професор Р. С. Орловський у своїх наукових дослідженнях акцентує увагу на фундаментальній проблемі визначення сутності суспільно небезпечних наслідків як категорії кримінального права, що не може бути зведена до суб'єктивного припущення або інтуїтивного сприйняття [21]. Він підкреслює, що загроза настання таких наслідків має об'єктивний характер, який проявляється у створенні конкретної ситуації, що закономірно призводить або може призвести до настання небажаних наслідків, передбачених нормами кримінального права. Ця ситуація формується внаслідок кримінально протиправної поведінки особи, тобто дій або бездіяльності, які порушують встановлені правові норми та створюють умови для реалізації небезпеки. Отже, загроза в даному контексті розглядається як об'єктивний юридичний факт, а не як суб'єктивне припущення або гіпотетичне передбачення.

У кримінально-правовій теорії такі правопорушення, які полягають у створенні загрози суспільним інтересам, отримали спеціальний термін — «делікти створення небезпеки». Цей підхід має важливе теоретичне та практичне значення, оскільки дозволяє розмежувати злочини, де результатом є безпосереднє заподіяння шкоди, та ті, де шкода потенційно можлива і виникає

внаслідок створення відповідних умов і обставин, що можуть у подальшому спричинити тяжкі наслідки [23].

Важливе доповнення до цієї позиції дає В. І. Борисов, який аргументує віднесення створення небезпеки до видів суспільно небезпечних наслідків тим, що у випадку настання такого результату змінюється зовнішня обстановка — виникають реальні, конкретні умови та сили, здатні при безперешкодному розвитку подій призвести до безпосередньої шкоди. Цей аргумент підкреслює причинно-наслідкову природу кримінально караного діяння, адже наявність реальної загрози формує потенціал для настання негативних результатів, які закон визначає як кримінально-правову шкоду.

У випадку терористичного акту, який передбачає застосування зброї, вчинення вибуху, підпалу чи інших дій, що створюють небезпеку для життя, здоров'я, майна або інших істотних суспільних цінностей, законодавець визначає його як кримінальне правопорушення із матеріальним складом, тобто «делікт небезпеки». Такий склад характеризується низкою складових елементів. По-перше, це альтернативність форм діянь, що включають різні способи реалізації терористичного акту — застосування зброї, вибухові пристрої, підпал, а також інші дії, здатні спричинити загрозу. По-друге, наявність наслідків у вигляді створення реальної небезпеки для життя або здоров'я, значної майнової шкоди чи інших тяжких наслідків, які мають бути встановлені об'єктивно. По-третє, необхідна наявність причинного зв'язку між діями винного та наслідками, тобто встановлення того, що саме ці дії закономірно спричинили створення небезпеки [3].

Визначення причинного зв'язку є ключовим для підтвердження наявності об'єктивної сторони злочину. Це вимагає застосування відповідних кримінально-правових і криміналістичних методів дослідження, що забезпечують доказування факту зв'язку між протиправною поведінкою та створенням небезпеки. Лише за наявності цього зв'язку можна говорити про вчинення саме кримінального правопорушення у формі терористичного акту з матеріальним складом, що диференціює його від інших злочинів, пов'язаних з насильством або шкодою, які не мають ознак створення об'єктивної загрози.

Поняття терористичних загроз належить до фундаментальних категорій кримінально-правової науки, а також є важливим інструментом для розуміння механізмів попередження і протидії терористичній діяльності на національному та міжнародному рівнях. В сучасній кримінології та безпекознавстві терористичні загрози розглядаються як потенційні або реально існуючі умови, що створюють небезпеку для суспільного ладу, безпеки держави, життя і здоров'я громадян, а також для функціонування інституцій влади [38]. Це складне явище, що має як об'єктивний, так і суб'єктивний виміри, що зумовлює необхідність комплексного аналізу його змісту, характеристик та юридичних наслідків.

Терористична загроза у правовому аспекті виступає як потенційна можливість здійснення терористичного акту або комплексу дій, спрямованих на заподіяння шкоди суспільству або державі. Вона не є абстрактним припущенням, а конкретним, об'єктивно існуючим станом речей, який характеризується наявністю певних умов, що можуть призвести до тяжких суспільно небезпечних наслідків [36]. Ці умови, згідно з кримінальною теорією, утворюють «делікти створення небезпеки», що означає факт фактичного виникнення ситуації, у якій суспільна безпека опиняється під реальною загрозою, незалежно від того, чи відбувся вже фактичний шкодочинний акт.

Об'єктивна сторона терористичних загроз проявляється у конкретних діях чи бездіяльності, що закономірно можуть призвести до реалізації терористичного акту. Під цими діями розуміють будь-які протиправні вчинки, які безпосередньо або опосередковано сприяють створенню атмосфери страху, паніки, порушення громадського порядку, наприклад, підготовка вибухових пристроїв, накопичення зброї, проведення вербувальних акцій серед населення, розповсюдження екстремістської ідеології [34]. Важливо підкреслити, що критерієм для оцінки дій як терористичної загрози є не лише їхня потенційна шкода, а й спрямованість на досягнення певної мети, що має політичний, релігійний, ідеологічний або інший характер, а також публічний характер цих дій, який забезпечує залучення уваги широких верств населення або органів влади.

Суб’єктивна сторона терористичних загроз охоплює усвідомлення особою суспільної небезпеки її поведінки, наявність умислу, спрямованого на досягнення терористичних цілей шляхом створення відповідної обстановки страху та залякування. Підсвідомий або випадковий характер дій виключає кваліфікацію їх як терористичних загроз. Для правової оцінки важливо встановити намір особи – цілеспрямовану поведінку, спрямовану на дестабілізацію суспільних відносин, примус органів влади чи населення до певних дій або утримання від них [33].

З огляду на функціональне призначення поняття терористичних загроз у правовій системі, воно має бути чітко сформульованим у законодавстві для забезпечення дієвості превентивних заходів. Законодавче визначення цього поняття повинно враховувати як кримінально-правові аспекти, що передбачають кримінальну відповідальність за створення умов для терористичної діяльності, так і адміністративно-правові норми, що регламентують порядок виявлення та нейтралізації загроз. Відсутність чітких критеріїв може призводити до політизації або зловживань при кваліфікації окремих діянь.

Інтеграція поняття терористичних загроз у практику боротьби з тероризмом вимагає тісної взаємодії кримінального законодавства, правоохоронних органів, органів національної безпеки та міжнародних структур [36]. Виявлення і аналіз загроз здійснюється на підставі збирання інформації з різних джерел, у тому числі оперативної, розвідувальної та аналітичної діяльності, що дозволяє своєчасно оцінити рівень ризику та вжити необхідних заходів. Науковий підхід до вивчення терористичних загроз передбачає розробку системи критеріїв їх класифікації, що включає фактори мотивації, методи здійснення, рівень суспільної небезпеки, можливі наслідки, а також категорії суб’єктів загроз [37].

Важливою характеристикою терористичних загроз є їх динамічність та мінливість, що зумовлено постійною трансформацією методів і засобів терористичної діяльності, а також змінністю політичного, соціального та інформаційного контексту. Сучасні технології, зокрема кібертероризм, використання безпілотних літальних апаратів, поширення екстремістських

ідеологій через інтернет, значно розширили арсенал засобів створення та реалізації терористичних загроз, що вимагає від правозахисних органів і науковців постійного оновлення знань, застосування міждисциплінарних підходів та використання інноваційних методів протидії [40].

Розглядаючи терористичні загрози з позиції кримінології, слід наголосити на важливості дослідження соціально-психологічних аспектів їх формування, зокрема впливу екстремістської ідеології, рівня соціальної напруженості, безробіття, міжнаціональних та міжрелігійних конфліктів. Ці фактори виступають як каталізатори виникнення і розвитку потенційних загроз, що в свою чергу підкреслює необхідність комплексного підходу до їх дослідження, включаючи соціальні, правові, політичні та психологічні аспекти.

У рамках класифікації за політичним критерієм подальші дослідники виокремили революційний, підреволюційний та репресивний тероризм. Революційний тероризм характеризується прагненням докорінної зміни політичної системи, часто шляхом насильницького повалення існуючого ладу і встановлення нового політичного устрою. Такий тероризм орієнтований на максимальне знищення старих інституцій і створення умов для радикальних соціально-політичних трансформацій. Підреволюційний тероризм, навпаки, має на меті здійснення певних змін в межах існуючої системи, не прагнучи до її повного знищення, а радше до корекції або реформування політичних структур. Репресивний тероризм відображає дії держави або її агентів, спрямовані на придушення політичної опозиції або підрив діяльності інших держав через застосування терористичних методів, що перетворює тероризм у засіб державної політики, який легітимізує насильство у політичних цілях [37].

Іншим способом класифікації терористичних організацій є поділ за ідеологічною орієнтацією на ліві та праві угруповання. Ліві терористичні організації зазвичай мають революційну ідеологію, спрямовану на докорінне перетворення суспільного ладу, часто шляхом насильницького усунення існуючих політичних структур. Вони можуть відстоювати ідеї соціальної справедливості, рівності, боротьби з капіталізмом або імперіалізмом. Такі групи часто апелюють до класової боротьби і масового визвольного руху, прагнучи

залучити широкі верстви населення [34]. Праві терористичні організації зазвичай мають консервативну, націоналістичну або фашистську ідеологію, орієнтовану на збереження або відновлення певних традиційних цінностей, державної цілісності або етнічної чистоти. Вони часто виступають проти імміграції, культурних змін, соціальної рівності, і їхня діяльність може бути спрямована на дискримінацію та насильство щодо певних соціальних чи етнічних груп.

Класифікація, що включає державний і опозиційний тероризм, дозволяє аналізувати різні суб'єкти терористичної діяльності з огляду на їх правовий статус і мету. Державний тероризм проявляється у застосуванні насильства державою або її агентами для утвердження своєї влади, придушення інакомислення, або впливу на внутрішню чи зовнішню політику. Опозиційний тероризм, навпаки, виникає як форма спротиву діючим режимам, часто в умовах політичної репресії або соціальної несправедливості. Така дихотомія допомагає зрозуміти природу конфлікту і правову оцінку відповідних дій, а також визначити правові механізми і політичні стратегії для їх вирішення.

Таким чином, систематизація терористичних дій та організацій за різними критеріями — мотиваційним, ідеологічним, політичним, економічним, соціальним та релігійним — сприяє формуванню цілісної картини феномену тероризму. Такий комплексний підхід дозволяє не лише розмежувати види тероризму за їх специфічними ознаками, а й розробити диференційовані стратегії протидії, що враховують особливості кожного типу, їх взаємозв'язки та трансформації в процесі глобалізації та змін у міжнародному середовищі.

Класифікаційні підходи до тероризму, які пропонуються сучасними науковцями, відображають складність і багатогранність цього соціально-політичного феномену, що перетинає межі кримінології, політичної науки, соціології та безпеки. Існуючі концепції класифікації терористичних проявів спрямовані на виділення специфічних ознак, що дозволяють розрізняти різні форми та види терористичних дій залежно від мотивації, методів, суб'єктів і цілей.

З-поміж широкого спектра підходів, один із них пропонує поділ тероризму на політико-соціальний та політико-релігійний. Такий поділ демонструє

взаємозв’язок між політичними цілями та додатковими ідеологічними або культурними чинниками, які обумовлюють вибір інструментів насильства. Політико-соціальний тероризм зазвичай пов’язаний із боротьбою за соціальні трансформації, ліквідацію нерівності чи несправедливості у суспільстві. Він часто виникає на базі класових, етнічних чи національних конфліктів, що мають глибокі соціальні корені [36]. Політико-релігійний тероризм, у свою чергу, опирається на релігійні доктрини або фанатичні інтерпретації релігії, які слугують як легітимація насильства та мобілізація послідовників для досягнення політичних чи ідеологічних цілей. Ця форма тероризму відзначається високим рівнем ідеологічної мотивації, жорстокістю та непередбачуваністю дій.

Інша модель класифікації пропонує виділення чотирьох різновидів тероризму: національного, одномірного, політичного і релігійного. Національний тероризм концентрується на прагненні певної етнічної або національної спільноти до самовизначення, автономії або незалежності, часто супроводжуючись етнонаціональними конфліктами та боротьбою за територіальний контроль. Одномірний тероризм має вузькоспеціалізовану спрямованість, де терористична діяльність фокусується на одній конкретній проблемі або меті, без ширшого політичного чи соціального контексту. Політичний тероризм більш загальний, орієнтований на зміну або вплив на політичні структури та процеси [44]. Релігійний тероризм базується на сакралізації боротьби, де релігійні переконання визначають як кінцеві цілі, так і методи насильства.

Ще один підхід передбачає класифікацію тероризму з огляду на приналежність до певних ідеологічних спектрів: тероризм держави лівих, держави правих, лівої опозиції і правої опозиції. Ця типологія відображає політичні вподобання та ідеологічні орієнтації суб’єктів терористичних дій, що є важливим для аналізу внутрішньої і зовнішньої політики, а також для виявлення потенційних джерел конфліктів. Ліві державні форми тероризму зазвичай пов’язані з авторитарними режимами, що використовують насильство для підтримки ідеології соціалізму чи комунізму. Праві державні терористичні практики часто базуються на фашистських або ультранаціоналістичних ідеях.

Опозиційний тероризм із лівого чи правого флангу відображає спротив існуючим режимам із відповідними ідеологічними переконаннями [38].

У сучасній науковій думці підкреслюється важливість розгляду субверзивного та підривного тероризму, які мають на меті дестабілізацію політичного ладу і підрив влади, використовуючи інструменти насильства як форму «збройної пропаганди». Ця форма тероризму спрямована не лише на фізичне знищення опонентів, а й на демонстрацію власної сили і можливостей потенційним союзникам, стимулюючи політичну мобілізацію та розширення впливу.

Поряд із політичними і соціальними аспектами, у сучасних умовах набуває поширення кримінальний тероризм, що пов’язаний із діяльністю організованих злочинних угруповань. Цей тип тероризму виконує функцію засобу впливу на конкуренцію в кримінальному світі, державні структури, правоохоронні органи з метою створення сприятливих умов для нелегальної діяльності. Кримінальний тероризм відрізняється від традиційних політико-ідеологічних форм відсутністю чітких політичних чи ідеологічних цілей, натомість він сконцентрований на економічних інтересах, контролі над ринками, ресурсами і територіями.

Транснаціональний тероризм є окремим викликом сучасності, оскільки він втілює перетікання інформації, капіталу, матеріальних ресурсів і кадрів через державні кордони, формуючи мережі, які виходять за межі національних юрисдикцій [38]. Цей вид тероризму ускладнює міжнародне співробітництво, створює загрози безпеці на глобальному рівні і вимагає нових підходів у правовому та оперативному реагуванні.

Також сучасні дослідники відзначають появу комерційного тероризму, що, по суті, є кримінальним тероризмом із акцентом на економічну вигоду, ідеологічного тероризму, що відповідає традиційним політичним, націоналістичним або релігійним формам, а також інформаційного тероризму — нового феномену, що полягає у використанні інформаційних технологій, пропаганди та кібернетичних атак для впливу на суспільну свідомість, дестабілізації державних інститутів та формування психологічного тиску.

Таким чином, багатогранність класифікаційних моделей відображає реалії сучасного терористичного руху, який постійно змінюється, інтегрує різноманітні мотиви, методи і форми дій. Наукове осмислення цих підходів дозволяє не лише уточнити теоретичні засади вивчення тероризму, а й сприяє розробці ефективних комплексних стратегій протидії, що враховують як традиційні, так і новітні прояви цього феномену.

Узагальнюючи, тероризм у XXI столітті є складним і багатогранним соціально-політичним феноменом, що вимагає глибокого наукового аналізу та комплексного підходу до протидії. Він характеризується динамічністю, транснаціональністю та здатністю адаптуватися до сучасних технологічних умов. Терористичні загрози мають складну структуру, що поєднує кримінальні, політичні, соціальні та психологічні аспекти, і потребують системної оцінки ризиків.

1.2. Основні методи оцінки ризиків тероризму

У сучасному глобалізованому суспільстві, в умовах постійного зростання загроз гібридного, транснаціонального та асиметричного характеру, поняття ризику тероризму набуває виключно важливого значення у сфері державної, регіональної та міжнародної безпеки. Тероризм як феномен XX–XXI століття трансформувався з локалізованого прояву насильства у високоорганізовану форму нелінітичного впливу, що здатна підривати стійкість політичних інститутів, дестабілізувати економіку, дезінтегрувати суспільства та спричиняти глибокі безпекові кризи. У цьому контексті виникає потреба в об’єктивному, концептуально структурованому та методологічно вивіреному підході до визначення і розуміння поняття ризику тероризму.

У науковому дискурсі термін «ризик тероризму» формується на основі міждисциплінарного підходу, який поєднує у собі елементи безпекознавства, соціології, кримінології, політології, стратегічних досліджень та системного аналізу. Згідно з домінуючим концептуальним підходом у сфері безпекових досліджень, ризик тероризму є функцією трьох основних змінних: ймовірності

реалізації терористичного акту, вразливості об’єкта впливу (інфраструктури, населення, інституцій) і потенційної шкоди, що може бути завдана внаслідок такої події [1]. Таким чином, ризик тероризму може бути формально представлений як взаємодія загроз, уразливостей та наслідків у рамках специфічного безпекового середовища.

Особливістю ризику тероризму, яка вирізняє його серед інших типів безпекових ризиків, є свідомий намір його ініціаторів завдати шкоди, використовуючи психологічний ефект терору як засіб досягнення стратегічних цілей. Це зумовлює потребу в урахуванні в аналізі ризику не лише матеріальних, а й нематеріальних аспектів — зокрема, когнітивних моделей сприйняття терористичної загрози суспільством, ступеня політичної дестабілізації, впливу на масову свідомість та соціальну поведінку. Таким чином, ризик тероризму постає як феномен, що поєднує в собі матеріальні загрози (фізичне знищення, руйнування інфраструктури), політичні наслідки (делегітимація влади, політична криза), інформаційно-психологічні ефекти (масова паніка, радикалізація) та економічні втрати (дестабілізація ринків, прямі матеріальні збитки).

Важливо також усвідомлювати, що ризик тероризму не є сталим у часі або просторі. Він формується під впливом широкого спектра чинників: геополітичного положення, ступеня соціально-економічної нерівності, політичної стабільності, ефективності інституційного управління, стану правоохоронної та розвідувальної системи, рівня інтеграції у глобальні комунікаційні мережі. Отже, кожна держава, кожен регіон і навіть кожен населений пункт має свою унікальну конфігурацію ризиків терористичного характеру, що потребує специфічного підходу до їх ідентифікації, класифікації та мінімізації [41].

Значне місце у визначенні ризику тероризму посідає категорія критичної інфраструктури, яка охоплює системи життєзабезпечення держави: енергетику, транспорт, водопостачання, охорону здоров’я, фінансову систему, цифрові комунікації. Терористичний акт, спрямований проти елементів цієї інфраструктури, має потенціал викликати не лише локальні руйнування, а й

системні збої, що загрожують національній стабільності [5]. Тому визначення ризику тероризму неможливе без глибокого аналізу вразливостей критичних об’єктів та потенційних ланцюгових реакцій, які можуть бути спровоковані внаслідок їх ураження.

У контексті сучасного розвитку систем безпеки як на національному, так і на міжнародному рівнях, проблема оцінки ризиків тероризму посідає ключове місце в процесі формування ефективної політики протидії терористичним загрозам. Системна оцінка ризиків є не лише інструментом аналітичного опрацювання актуальних загроз, але й фундаментальною складовою стратегічного планування, превентивного реагування та комплексного управління кризовими ситуаціями, спричиненими діяльністю терористичних суб’єктів [32]. Зважаючи на транснаціональний характер тероризму та його здатність адаптуватися до нових соціально-політичних і технологічних реалій, застосування адекватних механізмів ризик-менеджменту є визначальним чинником забезпечення стійкості держав до зовнішніх і внутрішніх деструктивних впливів.

Оцінка ризиків тероризму тісно пов’язана з доктринальними основами національної безпеки. У межах сучасних національних стратегій безпеки більшості демократичних країн, оцінка ризиків розглядається як ключовий етап циклу управління безпекою, що включає ідентифікацію загроз, аналіз уразливостей, оцінку потенційних наслідків та розробку заходів з мінімізації ризиків. Така структурна модель дозволяє інституціям сектору безпеки діяти проактивно, враховуючи не лише безпосередню ймовірність терористичних атак, але й ширший соціально-політичний контекст, в якому ці атаки можуть реалізовуватись. Оцінка ризиків, таким чином, виконує функцію не лише інструментальної підтримки, але й задає стратегічні параметри політики протидії.

Особливого значення набуває оцінка ризиків у контексті захисту критичної інфраструктури. Ідентифікація об’єктів, що є найбільш вразливими до терористичних посягань — енергетичні системи, транспортні вузли, фінансові інституції, інформаційно-комунікаційні мережі, водопостачання тощо —

дозволяє організовувати політику захисту на основі принципу пріоритетності та ефективного розподілу ресурсів [33]. У цьому разі оцінка ризиків не обмежується аналізом ймовірності атаки, але включає в себе детальний аналіз системних наслідків ураження того чи іншого елементу інфраструктури. Саме тому у сучасних західних підходах особливу увагу приділяють сценарному моделюванню криз, в рамках якого ризик оцінюється через призму системної вразливості держави як цілісного соціального організму.

Важливою складовою ефективної оцінки ризиків у системі протидії тероризму є її інтеграція в інформаційні політики. Суспільна комунікація щодо терористичних загроз, побудована на базі об'єктивних, науково вивірених даних, дозволяє уникати як паніки, так і байдужості, формуючи раціональне сприйняття ризику у громадян. У свою чергу, це створює передумови для ефективної взаємодії населення з державними інституціями, зниження рівня радикалізації, а також формування культури безпеки на всіх рівнях суспільства.

Узагальнюючи, роль оцінки ризиків у системі національної та міжнародної безпеки є системоутворювальною. Вона виступає як методологічна, управлінська та інформаційна основа для формування політики протидії терористичній загрозі. Її інтеграція в процеси стратегічного планування, кризового управління, комунікаційної політики та міжнародного співробітництва дозволяє не лише своєчасно ідентифікувати загрози, а й ефективно реагувати на них, забезпечуючи стійкість держави та суспільства до зовнішніх і внутрішніх дестабілізуючих впливів.

Оцінка ризиків тероризму як складовий елемент системи національної та міжнародної безпеки має фундаментальне значення в процесі управління загрозами, прогнозування кризових ситуацій і забезпечення ефективної реалізації превентивних заходів. Зважаючи на багатоаспектність терористичної загрози, що охоплює соціальні, політичні, економічні, релігійні та технологічні виміри, методи оцінювання ризиків повинні відповідати рівню складності аналізованого об'єкта [23]. Саме тому у сфері дослідження ризиків тероризму склалась система підходів, яка умовно поділяється на кількісні, якісні та комбіновані (інтегративні) методи. Кожен із зазначених підходів має свої

специфічні ознаки, методологічні основи та практичне значення для побудови ефективних моделей реагування на терористичну загрозу.

Кількісні методи оцінки ризиків тероризму ґрунтуються на формалізованих підходах до обробки емпіричних даних з використанням статистичних, математичних і логіко-числових моделей. Основна мета цих методів полягає у визначенні ймовірності реалізації загроз, ступеня уразливості об’єктів потенційного терористичного впливу та очікуваного масштабу наслідків [22]. Застосування кількісного інструментарію дозволяє отримати об'єктивовані, числово виражені показники, які можуть бути використані для порівняльного аналізу, ранжування ризиків, розрахунку сценаріїв розвитку подій та формування нормативних критеріїв допустимого ризику.

Якісні методи оцінки ризиків тероризму будуються на інтерпретативному підході до аналізу загроз, де основним аналітичним інструментом виступають експертні оцінки, сценарний аналіз, контекстуальне моделювання та соціополітичне прогнозування. Цей клас методів надає особливої уваги контексту — геополітичному, культурному, правовому, релігійному, комунікаційному тощо. Саме якісні методи дозволяють глибше осягнути мотивацію терористичних акторів, ідеологічні передумови радикалізації, специфіку регіональних терористичних мереж, соціальні аспекти сприйняття терору та реакції населення [23].

Одним із ключових методів цього підходу є метод експертного оцінювання, який полягає у залученні фахівців різного профілю — від антитерористичних служб до філософів, соціологів, релігієзнавців — з метою формування цілісної картини ризику. Методології типу Delphi або SWIFT (Structured What-If Technique) забезпечують системність експертного мислення, мінімізують упередження та формують консенсусні оцінки. Застосування якісного аналізу виправдане у випадках, коли брак даних або специфічність ситуації унеможливлює математичну формалізацію [29]. Водночас недоліком таких методів є їх суб’єктивність, яка, попри використання методологічних фільтрів, залишається вагомим чинником впливу на результативність оцінки.

Якісні методи широко використовуються в рамках аналізу уразливості критичної інфраструктури, інформаційного простору, виявлення ознак радикалізації у медіа-дискурсі та в соціальних мережах. Зважаючи на зростання ролі кіберпростору в координації терористичних актів, саме якісний підхід дозволяє ідентифікувати небезпечні наративи, виявляти ризикогенні спільноти та оперативно реагувати на інформаційні атаки. Цей клас методів також дає змогу здійснювати етноконфесійну, етнополітичну, культурологічну оцінку ризиків, що є критично важливим у мультикультурних суспільствах та прикордонних регіонах [29].

Комбіновані або інтегративні підходи до оцінки ризиків тероризму є найбільш гнучкими та адаптивними, адже поєднують сильні сторони як кількісних, так і якісних методів. Основна ідея полягає в консолідації статистичного аналізу з експертним знанням, що дозволяє досягнути більшої точності, валідності та практичної релевантності оцінки ризиків [1]. Інтегративні моделі враховують і об'єктивні, і суб'єктивні чинники ризику, що, своєю чергою, робить їх ефективними в умовах швидкозмінного середовища загроз.

Інтегративні методи є базовими у створенні комплексних інформаційно-аналітичних систем моніторингу безпеки, у межах яких поєднуються дані з відкритих джерел, агентурної розвідки, кіберрозвідки та аналітичної обробки експертами. У таких системах ризик тероризму оцінюється не лише як результат однієї події, а як функція системної взаємодії різних елементів безпекового середовища. Це дає змогу прогнозувати не лише індивідуальні атаки, але й стратегічні зміни в структурі терористичних загроз, рівень їхньої адаптивності та загальну конфігурацію ризиків у глобальному контексті.

Використання індикаторних моделей ризику передбачає побудову системи показників, які можуть виступати маркерами ймовірного посилення терористичної загрози в певному середовищі. Ці індикатори класифікуються за типологією: політичні (зростання політичної напруги, делегітимація влади), соціальні (ріст протестної активності, зростання безробіття серед молоді), культурні (радікалізація через релігійні громади), інформаційні (зростання ворожих меседжів у соціальних мережах), безпекові (активація нелегальних

потоків зброї або вибухових речовин). Індикаторний підхід дозволяє розробляти динамічні карти ризику, оновлювані в режимі реального часу, та здійснювати попереджувальний моніторинг середовища. У свою чергу, кожен індикатор може бути об’єктом оцінки через експертну валідацію, а також порівняльний аналіз у міжрегіональному вимірі.

Геопросторовий аналіз ризиків тероризму як елемент кількісної методології базується на використанні геоінформаційних систем (ГІС) і картографічних даних для візуалізації просторового розподілу загроз, уразливих об’єктів та динаміки розвитку ризикових подій. Цей підхід дозволяє інтегрувати інформацію з різних джерел — супутникові знімки, дані соціальних мереж, дані поліції та розвідки — з метою визначення географічно зосереджених кластерів ризику. Геоаналіз є надзвичайно ефективним інструментом для розміщення ресурсів безпеки, побудови маршрутів патрулювання, вибору місць розміщення інфраструктури безпеки (камер спостереження, блокпостів, укриттів). Його також використовують при оцінці ризиків, пов’язаних із транспортуванням небезпечних вантажів або забезпеченням масових заходів [25].

SWOT-аналіз терористичних загроз виступає ефективним інструментом виявлення сильних та слабких сторін існуючих систем безпеки, а також можливостей і загроз у зовнішньому середовищі. Цей метод дозволяє сформулювати стратегічні напрями вдосконалення безпекових політик через системне порівняння внутрішніх характеристик системи безпеки (наявність професійного персоналу, ресурсне забезпечення, технологічна інфраструктура) з зовнішніми чинниками ризику (поява нових радикальних угруповань, зміна геополітичного контексту, поширення нелегального озброєння). SWOT-аналіз забезпечує міждисциплінарну платформу для взаємодії представників уряду, силових структур, експертного середовища та громадянського суспільства, а його результати можуть бути включені до національних стратегій або операційних планів.

Аналіз уразливості критичної інфраструктури є невід’ємною складовою якісної оцінки ризиків тероризму, адже він дозволяє ідентифікувати об’єкти, знищення або пошкодження яких може мати катастрофічні наслідки для

національної або регіональної безпеки. Такий аналіз охоплює вивчення енергетичних систем, водопостачання, транспортних вузлів, об’єктів телекомунікацій, охорони здоров’я, банківської інфраструктури. У ході аналізу розглядаються не лише фізичні аспекти уразливості, але й кібернетичні, управлінські, соціальні. До уваги беруться такі параметри, як доступність, ступінь захищеності, можливість резервного функціонування, рівень підготовки персоналу, що дозволяє формувати карти уразливості, розробляти пріоритети фінансування заходів із захисту, планувати сценарії реагування на надзвичайні ситуації.

У сукупності кількісні й якісні методи оцінки ризиків формують багаторівневу аналітичну платформу для ефективного управління терористичними загрозами. Вони дозволяють не лише виявляти джерела ризику, але й адаптувати безпекову політику до нових викликів, що виникають у динамічному середовищі сучасного глобалізованого світу.

У рамках сучасної парадигми забезпечення національної та міжнародної безпеки особливу роль відіграють моделі, що дозволяють здійснювати системну, об'єктивну та релевантну оцінку ризиків терористичної активності. Однією з таких високоефективних моделей є методика CARVER, яка походить із військової практики Сполучених Штатів і широко адаптована до потреб цивільної безпеки, зокрема у сфері захисту критичної інфраструктури. Ця модель передбачає комплексну оцінку потенційної цілі терористичної атаки за шістьма критеріями: критичність (Criticality), доступність (Accessibility), відновлюваність (Recuperability), уразливість (Vulnerability), ефект (Effect), можливість розпізнавання цілі (Recognizability). Кожен з параметрів має шкалу оцінювання, що дозволяє формалізувати ризики у кількісній формі та виявити об’єкти, що потребують першочергового захисту [25]. Особливість підходу CARVER полягає в його мультидисциплінарності: він об'єднує елементи військової доктрини, об'єктивної експертної оцінки та тактичного прогнозування. У контексті антитерористичної діяльності модель дозволяє оперативно реагувати на зміни у зовнішньому середовищі, забезпечуючи динамічну переоцінку пріоритетів у захисті об’єктів.

Системна перевага CARVER полягає у її адаптивності: модель може бути використана як у локальному контексті — наприклад, при охороні важливих транспортних вузлів, енергетичних об’єктів чи урядових установ — так і в більш широкому стратегічному контексті, при розробці національних програм безпеки. Слід підкреслити, що така модель особливо цінна в умовах гібридного характеру сучасного тероризму, де класичні фізичні атаки поєднуються з кіберзагрозами, інформаційними впливами, біологічним чи хімічним тероризмом. Сегментована структура CARVER дозволяє оцінювати кожен тип загроз в окремому аспекті, формуючи зважений інтегральний ризиковий індекс.

Ще однією з передових сучасних методик оцінювання ризиків у сфері боротьби з тероризмом є система TVRA (Threat, Vulnerability, and Risk Assessment), що походить із практики корпоративної безпеки, але набула широкого вжитку у державних інституціях, зокрема в сфері охорони критичних об’єктів інфраструктури. TVRA реалізує триетапний процес: по-перше, визначення джерел загроз (threat assessment) із урахуванням їхніх намірів, можливостей та історичного контексту; по-друге, аналіз вразливостей (vulnerability assessment), що охоплює як фізичні, так і кібернетичні компоненти безпеки; по-третє, інтеграція обох елементів в оцінку ризику (risk assessment), яка включає ймовірність реалізації загрози та тяжкість її наслідків. Така структурна чіткість робить TVRA інструментом із високою аналітичною потужністю, що дозволяє використовувати його не лише для ретроспективного аналізу, але й для прогнозування майбутніх викликів.

Методологічною перевагою TVRA є її гнучкість і адаптивність до нових загроз, включно з транснаціональним тероризмом, кібератаками, інсайдерськими загрозами в межах закритих об'єктів. У сучасному безпековому середовищі, що характеризується надзвичайно високим рівнем динамізму та асиметрії, TVRA дозволяє впроваджувати механізми проактивної протидії ризикам на основі контекстуалізованого аналізу даних. Важливо також, що в рамках цієї методики широко використовується візуалізація результатів — графи, матриці ризику, діаграми сценаріїв, що сприяє кращому сприйняттю інформації керівництвом та оперативному прийняттю управлінських рішень.

Особливу увагу в сучасних підходах до оцінки ризиків у сфері боротьби з тероризмом привертають інтегровані інформаційно-аналітичні платформи, до яких входять системи, що поєднують машинне навчання, штучний інтелект (ШІ), великі дані (Big Data), хмарні обчислення та аналітику в режимі реального часу. Такі платформи дають змогу здійснювати динамічне, багаторівневе моделювання загроз, з урахуванням не лише структурних змін у середовищі безпеки, але й поведінкових та культурних чинників. Використання систем штучного інтелекту в цьому контексті ґрунтується на здатності алгоритмів виявляти приховані кореляції між подіями, ідентифікувати патерни, які передують терористичним актам, та автоматично оновлювати моделі ризиків відповідно до змінних параметрів.

Зокрема, машинне навчання застосовується для аналізу масивів інформації з відкритих джерел (OSINT), включаючи соціальні мережі, новинні агрегатори, форуми, блоги, які можуть бути використані терористичними структурами для вербування, поширення ідеології або координації дій. Індикатори, отримані в результаті автоматизованого збору та обробки даних, дозволяють формувати предиктивні моделі, що дають змогу прогнозувати не лише ймовірність атак, але й потенційні географічні та соціальні вектори їх реалізації. Перевага використання ШІ в оцінці ризиків полягає у його здатності до самонавчання: алгоритми, аналізуючи результативність власних прогнозів, оптимізують моделі та підвищують точність оцінки ризиків у реальному часі.

Інтегровані аналітичні платформи забезпечують також можливість візуалізації складних моделей ризику через інтерфейси з графічними панелями, що є особливо актуальним для управлінських структур, які повинні оперативно приймати рішення. Такі панелі включають теплові карти, мережеві графи, часові діаграми, що дозволяє унаочнити ризики й оптимізувати розподіл сил безпеки. Застосування таких рішень вже реалізується в низці країн — наприклад, у США система Fusion Centers інтегрує дані з багатьох джерел з метою виявлення та профілактики терористичних загроз, у ЄС активно розвивається ініціатива EUROSUR із побудови єдиної платформи прикордонної безпеки, яка включає в себе елементи прогнозування ризиків, зокрема терористичних [25].

У процесі впровадження й розвитку сучасних методик оцінки ризиків терористичних загроз неминуче постають фундаментальні обмеження, які детермінують як точність результатів, так і їхню ефективність у прикладному вимірі. Серед найбільш критичних із них виокремлюється проблема обмеженого доступу до достовірних, структурованих і релевантних даних, що унеможливлює повноцінну реалізацію як кількісних, так і якісних методологічних підходів. В умовах, коли значна частина інформації про терористичні організації, їхні мережі, маршрути фінансування, схеми радикалізації та вербування класифікується як така, що має обмежений або секретний характер, академічне та цивільне середовище безпеки стикається з суттєвими викликами у процесі аналізу. Обмеження у доступі до розвідданих, оперативних зведень, досьє суб'єктів загроз та внутрішніх звітів призводить до фрагментарності аналітики, підвищення рівня умовності оцінок та небезпеки помилкових висновків.

У сфері відкритих джерел (OSINT) також фіксується ряд суттєвих проблем — насамперед, це низький рівень структурованості даних, наявність значного інформаційного шуму, тенденція до маніпулятивного впливу, а також значні обсяги дезінформації, поширюваної як терористичними осередками, так і іншими деструктивними агентами [27]. Для коректної фільтрації, інтерпретації та верифікації таких даних необхідні високоспеціалізовані технології обробки природної мови, синтаксичного аналізу та інтероперабельності між інформаційними платформами — вимоги, які часто залишаються недоступними для багатьох урядових структур, не кажучи вже про академічну спільноту. Також варто зазначити, що навіть при наявності технічного ресурсу, правові обмеження на міждержавний обмін даними, закони про конфіденційність, кіберетика та обмеження з боку приватних технологічних платформ становлять серйозні бар'єри для формування повноцінної картини ризиків.

Одним із найбільш складних викликів, що ускладнює моделювання терористичних ризиків, виступає надзвичайно динамічний і трансформаційний характер самих загроз. Тероризм сучасності — це феномен, що не має сталої організаційної, ідеологічної чи тактичної структури. Його еволюція від централізованих ієрархічних мереж до децентралізованих клітин, зокрема в

кіберпросторі, унеможливлює лінійне прогнозування. Застосування класичних статистичних моделей у такому контексті втрачає ефективність, адже вхідні параметри ризику постійно змінюються. Водночас новітні технології, що дозволяють динамічно оновлювати моделі на основі штучного інтелекту або самоорганізовуваних нейронних мереж, мають суттєву ваду — вони оперують історичними даними, які не завжди адекватно відображають майбутні типи загроз [17].

Таким чином, сучасна практика оцінювання ризиків тероризму розгортається в полі численних викликів — від технологічних і методологічних до політичних і гуманітарно-правових. Її ефективність напряму залежить не лише від точності інструментів чи обсягу доступної інформації, але й від рівня правової гнучкості, етичної виваженості та політичної волі до впровадження системного, аполітичного та об’єктивного підходу до протидії терористичним загрозам.

Отже, у сучасному глобалізованому світі оцінка ризиків тероризму є критично важливою для забезпечення національної та міжнародної безпеки. Цей процес включає використання кількісних, якісних та інтегративних методів, що дозволяють аналізувати ймовірність терористичних загроз, уразливість об'єктів та потенційні наслідки атак.

Висновки до розділу 1

У межах проведеного дослідження першого розділу магістерської роботи досліджено сутнісні характеристики тероризму як суспільно небезпечного соціально-правового явища, що проявляється у різних формах насильницької дії, спрямованої на досягнення політичних, ідеологічних, релігійних або інших цілей. На основі аналізу законодавчих актів, наукових позицій та міжнародно-правових документів встановлено, що поняття терористичної загрози, терористичного акту та тероризму загалом є багатовимірними і такими, що охоплюють як юридичний, так і політико-соціальний, етичний, безпековий і культурний виміри.

Виокремлено ключові підходи до дефініювання терористичної діяльності в національному правовому полі, зокрема у положеннях Закону України «Про боротьбу з тероризмом», а також у Кримінальному кодексі України, де міститься визначення терористичного акту в статті 258. Зіставлення нормативних та доктринальних трактувань дозволило визначити ряд суперечностей і теоретичних лакун, пов'язаних із відсутністю чітких меж між поняттями тероризму, терористичного акту, терористичної організації, а також відсутністю чіткого методологічного критерію для відмежування цих явищ від суміжних складів злочинів (диверсії, злочини проти громадського порядку, збройні заколоти тощо).

Встановлено, що сучасна національна правова система перебуває у процесі концептуального і правового оновлення під впливом трансформаційних змін у природі терористичних загроз, що набувають дедалі складнішого, динамічного і гібридного характеру. Особливої уваги заслуговує той факт, що терористичні акти дедалі частіше мають не лише фізичну, але й кібернетичну форму, що створює нові виклики для кримінально-правової кваліфікації та визначення складу злочину. У зв'язку з цим визначено необхідність глибшого міждисциплінарного осмислення тероризму як складного правового, соціального та безпекового феномену, який потребує синтезу правових, політологічних, соціологічних, антропологічних і філософських знань.

У результаті аналізу сучасних наукових підходів до класифікації терористичних загроз виокремлено політичний, релігійний, соціально-економічний та культурний виміри, кожен з яких має власну специфіку формування, прояву і функціонування. Зокрема, встановлено, що релігійно-мотивований тероризм часто використовує символічний простір та апеляції до сакральних ідеалів, тоді як політично вмотивований тероризм спрямовується на дестабілізацію легітимності інституційної влади та підрив державної стабільності. Досліджено взаємозв'язок між ідеологічними основами терористичної діяльності та радикалізацією населення, а також встановлено роль інформаційного простору у процесі вербування та мобілізації потенційних суб'єктів терористичних актів.

Розглянуто питання співвідношення загального поняття тероризму та його конкретного прояву — терористичного акту. Виокремлено, що останній є одиничним, конкретизованим кримінальним діянням, який за своїм змістом завжди має публічний характер, пов’язаний із демонстративним насильством і спрямованістю на широке соціальне, політичне або інформаційне охоплення. Досліджено, що склад терористичного злочину має матеріальну структуру і формується не лише фактом вчинення небезпечного діяння, але й створенням реальної загрози для життя, здоров’я, громадської безпеки, а також досягненням мети впливу на прийняття рішень органами влади чи місцевого самоврядування. Підтверджено, що для юридично коректної кваліфікації терористичних дій необхідним є встановлення не лише об'єктивної сторони, але й наявності цільової, мотиваційної та суб’єктивної складової.

Особливу увагу приділено концепції «деліктів створення небезпеки» як базовій для осмислення терористичних актів у контексті сучасної кримінально-правової теорії. Встановлено, що терористичні злочини, як правило, відносяться до групи злочинів із підвищеною суспільною небезпекою, що обґрунтовує необхідність посиленої кримінально-правової реакції, а також впровадження превентивних механізмів запобігання, включаючи оперативно-розшукові заходи, інформаційно-аналітичне моделювання та антикризове управління.

У процесі опрацювання наукових джерел також досліджено, що правозастосовна практика часто стикається з труднощами в ідентифікації цілей, мотивів, суб’єктів і організаційних структур терористичної діяльності, що зумовлює необхідність у подальшому вдосконаленні законодавчих конструкцій, формуванні чітких дефініцій та адаптації термінології до змін у характері загроз. Виокремлено потребу в перегляді та систематизації кримінально-правових норм, пов’язаних із боротьбою з тероризмом, для підвищення їхньої ефективності в умовах актуалізації гібридних загроз.

Загалом, у ході дослідження встановлено, що проблема тероризму є не лише юридичною, але й безпековою, політичною та соціальною категорією, що вимагає міждисциплінарного підходу до її розуміння, аналізу та протидії. Визначено, що сучасна система кримінально-правового реагування потребує

удосконалення, з урахуванням актуальних форм і методів терористичної діяльності, а також реалій глобальної безпеки. Це створює підґрунтя для подальших теоретичних і прикладних досліджень у наступних розділах даної роботи.

РОЗДІЛ 2. АНАЛІЗ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ ОЦІНКИ РИЗИКІВ ТЕРОРИЗМУ В УКРАЇНІ

2.1. Аналіз поточного стану терористичних загроз в Україні

Безпекове середовище України на сучасному етапі функціонує в умовах системної дестабілізації, яка зумовлена багатовимірним і багаторівневим

характером гібридної війни, що розгортається проти неї з 2014 року. Основу цієї конфліктної реальності складає поєднання класичних і неконвенційних форм агресії, включно з військовими, інформаційними, кібератакувальними, економічними та терористичними компонентами. Саме тому оцінка поточного стану безпеки держави потребує врахування як зовнішніх, так і внутрішніх факторів впливу, які формують складну, динамічну та конфліктогенну структуру загроз. В умовах, коли лінії фронту є не лише географічними, але й ментальними, комунікативними та кібернетичними, актуальним є міждисциплінарний аналіз безпекової ситуації, який передбачає врахування політичного, соціального, психологічного та правового контекстів.

Збройна агресія проти України не лише трансформувала архітектуру національної безпеки, а й спричинила сутнісну зміну самої природи загроз, які постали перед українською державністю. Воєнний стан, що триває, є не лише суто військовим протистоянням, але і системною кампанією із підриву політичної легітимності, руйнування соціального консенсусу, економічного виснаження, деморалізації населення та дискредитації національних інституцій. У межах такої стратегії особливого значення набуває застосування терористичних засобів і методів, які органічно вписуються у парадигму гібридної війни як інструмент впливу на критичну інфраструкуру, інформаційний простір, свідомість громадян і стратегічні рішення уряду [25].

Однією з ключових характеристик безпекового середовища є високий ступінь непередбачуваності, обумовлений систематичним порушенням правил ведення війни, широким використанням проксі-структур і диверсійно-розвідувальних груп, а також акцентом на невизнаних і неконвенційних формах втручання. Операції, що здійснюються під прикриттям, включаючи терористичні акти, спрямовані на підрив довіри до владних інституцій, дестабілізацію мирних регіонів, створення атмосфери страху та хаосу серед населення. Така ситуація унеможливлює застосування класичних підходів до протидії загрозам і вимагає системної адаптації інституційної спроможності держави [28].

Особливої уваги вартує те, що в умовах гібридної агресії тероризм виступає не як автономне явище, а як структурно інтегрована складова

комплексного впливу на державу. Терористичні дії координуються з інформаційно-психологічними операціями, маніпуляціями у соціальних мережах, розповсюдженням фейкових наративів і цілеспрямованим знищенням комунікаційних каналів. Таким чином, тероризм у сучасному українському безпековому контексті не є лише фізичним актом насильства, а виявляється у більш широкому контексті — як інструмент інформаційно-символічного контролю, спрямованого на формування в суспільстві параної, дезорієнтації, недовіри до держави та психологічної втоми [2].

Насамперед варто зазначити, що у воєнних умовах терористична активність є стратегічно зумовленою і цілеспрямованою [17]. Терористичні атаки, здійснені у глибокому тилу або у відносно мирних регіонах, переслідують не лише тактичну мету — завдання матеріальної шкоди чи дестабілізації ситуації в конкретному місті чи районі — а насамперед функціонують як інструмент системного руйнування загальнонаціональної стабільності. У структурі такої терористичної активності особливої ролі набувають акти саботажу, підриви елементів критичної інфраструктури, спроби отруєння водних джерел, підпали адміністративних або логістичних об'єктів, а також замахи на лідерів громадської думки та представників військово-цивільного адміністрування [17].

Особливу небезпеку становлять форми тероризму, які мають гібридну природу, тобто поєднують елементи звичайного криміналу, інформаційної війни та відкритих насильницьких дій. У воєнний час такі форми знаходять сприятливе середовище для розвитку, зокрема через підвищену міграційну мобільність населення, недостатню перевірку осіб, що перетинають лінії зіткнення, а також наявність великої кількості озброєння у неконтрольованому обігу. Застосування так званих «сплячих осередків» терористичних груп, які до певного моменту не проявляють жодної активності, але здатні за наказом активуватися у критичний момент, є типовим прийомом ведення асиметричної війни у воєнних умовах. Наявність таких осередків значно ускладнює роботу правоохоронних органів, оскільки ідентифікувати терориста до моменту його дії практично неможливо [30].

Ескалація терористичної активності в умовах воєнного стану тісно пов’язана з діями ворога, спрямованими на інспірацію соціальної паніки та делегітимацію центральної влади. Метою таких актів є підрив морально-психологічного стану громадян, створення атмосфери невпевненості, формування уявлення про безсилля держави перед обличчям загроз [1]. З цією метою використовуються як реальні насильницькі дії, так і погрози терористичного характеру, які спрямовані на паралізацію громадського життя. Акти інформаційного терору — масові повідомлення про мінування, фейкові новини про підготовку терактів, дезінформаційні кампанії у соціальних мережах — є частиною ширшої стратегії зламу суспільного опору.

Не менш важливим аспектом є адаптація форм і засобів здійснення терористичної діяльності до умов воєнного стану. Ворог активно використовує новітні технології, зокрема безпілотні літальні апарати (БПЛА), дистанційно керовані вибухові пристрої, пристрої віддаленого доступу до енергетичних систем та елементів управління. Крім того, зростає значення кібертехнологій у плануванні й реалізації терористичних загроз. В умовах воєнного стану, коли функціонування багатьох державних систем переведено на надзвичайний режим, такі атаки можуть бути особливо руйнівними, оскільки спричиняють перебої в електропостачанні, транспортному русі, роботі медичних установ чи органів місцевого самоврядування [1].

Значну увагу привертає також факт, що у воєнний період у держави зростає залежність від стратегічної інфраструктури — вузлів зв’язку, логістичних центрів, залізничних сполучень, паливно-енергетичних об’єктів. Саме ці об’єкти стають пріоритетною мішенню терористичних дій, особливо з боку ворожих ДРГ, що діють у тилу або в прифронтових районах. Руйнування такої інфраструктури має не лише локальні, але й загальнодержавні наслідки, порушуючи ланцюги постачання, гуманітарну логістику та систему мобілізації [17].

На тлі зазначених викликів актуалізується завдання постійного аналізу й переоцінки ризиків терористичної активності, що передбачає адаптацію аналітичних моделей до умов воєнного стану, формування нових сценаріїв

реагування, активізацію міжвідомчої координації та розбудову стратегічних центрів кризового управління. Ескалація терористичних загроз у контексті війни є системним феноменом, що охоплює не лише фізичну сферу безпеки, але й інформаційне середовище, соціальні практики, правове регулювання та психологічну стійкість населення [9]. Для ефективної протидії такій багатошаровій загрозі потрібна не лише модернізація правових механізмів, а й міждисциплінарна мобілізація наукового, технічного, комунікаційного й соціального потенціалу держави.

Функціонування диверсійно-розвідувальних груп (ДРГ) у сучасних умовах воєнного конфлікту на території України набуло масштабного та системного характеру, що обумовлює необхідність комплексного наукового аналізу цього явища як форми цілеспрямованої терористичної активності. ДРГ, будучи інструментом асиметричної війни, поєднують у собі елементи військової тактики, підпільної агентурної діяльності та терористичних методів ведення бойових дій. Унаслідок дії таких формувань зазнає підриву як обороноздатність держави, так і цілісність її соціальної, економічної, комунікаційної й інформаційної інфраструктури. В умовах повномасштабного збройного протистояння, поєднаного з режимом воєнного стану, ДРГ перетворюються на один з ключових інструментів гібридної агресії, спрямованої на зниження внутрішньої стійкості держави та підрив довіри до сил безпеки [11].

Основною ознакою диверсійно-розвідувальних груп є їхня здатність діяти на глибокій території противника, в умовах суворої секретності, із застосуванням методів маскування, легендування, а також тактик психологічного впливу. Формування, підготовка та застосування ДРГ відбувається за класичними принципами ведення спеціальних операцій: з урахуванням завдань з дестабілізації тилу, деморалізації цивільного населення, порушення логістичних каналів, знищення стратегічно важливих об’єктів або збирання розвідданих. Водночас ці завдання у своїй реалізації часто супроводжуються актами терору — цілеспрямованими підривами цивільної інфраструктури, підпалами адміністративних будівель, знищенням транспортних вузлів, енергетичних об’єктів, скоєнням убивств або замахів на представників державної влади.

Відмінність ДРГ від класичних військових підрозділів полягає у специфіці їх організації та методів діяльності. Такі групи, як правило, малочисельні, добре підготовлені в умовах дії поза тилом, мобільні й автономні. Вони оснащені сучасними засобами зв’язку, навігації, дистанційного спостереження, а також мають інструментарій для здійснення підривних робіт, мінування, дистанційного знищення цілей. У розрізі терористичних загроз їхню діяльність характеризує високий ступінь вибірковості мішеней: удари завдаються не тільки по військових об'єктах, але й по цивільному населенню, житловим будинкам, школам, лікарням, об'єктам енергозабезпечення та водопостачання — тобто усім тим елементам, що мають вирішальне значення для нормального функціонування держави в умовах воєнного часу.

Особливу увагу необхідно приділити тактичній зміні діяльності ДРГ у залежності від оперативної обстановки. Наприклад, у регіонах, що знаходяться поблизу лінії бойового зіткнення, ДРГ орієнтуються переважно на збір інформації про розташування військових підрозділів, спостереження за пересуванням техніки, коригування вогню артилерії або засобів ураження. У той час як у віддалених від фронту регіонах ці групи виконують завдання зі здійснення вибухів на інфраструктурних об’єктах, організації масових підпалів або підготовки терактів у місцях масового скупчення людей, зокрема на вокзалах, ринках, у навчальних закладах.

Особливості правового реагування на діяльність ДРГ зумовлюються складністю їх ідентифікації у контексті міжнародного гуманітарного права. Часто такі суб’єкти не носять встановленої військової форми, не мають чіткої ієрархічної структури та діють поза межами традиційного театру бойових дій. Це створює колізії при кваліфікації їхніх дій як воєнних злочинів або як терористичних актів. Відповідно, виникає потреба в удосконаленні нормативної бази, включно з адаптацією кримінального законодавства до сучасних форм гібридної агресії, формалізацією поняття диверсійної діяльності як складової тероризму, та створенням уніфікованих процедур для розслідування, збору доказів і подальшого притягнення до відповідальності.

В умовах сучасної воєнної конфігурації України ДРГ не просто виконують завдання зі збору розвідданих чи здійснення диверсій — вони є носіями терористичної логіки впливу на державу і суспільство. Їхня активність спрямована на створення стану постійної дестабілізації, порушення соціального контролю, руйнування цілісності простору безпеки. ДРГ стають мобільною, високоефективною формою інструменталізованого тероризму, що маскується під воєнну необхідність, але виявляє чіткі ознаки дій, які мають на меті не лише військовий результат, а й стратегічне підривання національного опору, психологічного стану суспільства та легітимності української державності як такої.

Такий тип діяльності вимагає від українських силових і аналітичних структур постійного оновлення системи реагування — не лише в сенсі тактичної протидії, але й у царині стратегічного мислення. Необхідно формувати моделі виявлення, прогнозування та нейтралізації ДРГ на основі сучасних інформаційних технологій, геоінформаційних систем, моделювання ризиків і глибокого аналізу соціальних процесів. Лише таким чином можливо забезпечити ефективне протистояння тій формі тероризму, яка водночас є мобільною, неформальною та системно небезпечною.

Оцінка каналів фінансування та матеріального забезпечення терористичних структур потребує ґрунтовного системного аналізу з позицій міждисциплінарного підходу, що поєднує кримінологічні, фінансово-економічні, безпекові та міжнародно-правові аспекти. Фінансування тероризму становить собою надзвичайно динамічний і складний феномен, що забезпечує життєздатність терористичних угруповань і трансформує окремі злочинні дії у стійку інфраструктуру загроз [1]. У сучасних умовах розгортання збройного конфлікту на території України, питання фінансового забезпечення тероризму набуває особливої гостроти, оскільки включає в себе як внутрішні, так і транснаціональні джерела ресурсів, які спрямовуються на підрив державної безпеки.

У контексті гібридної агресії, що реалізується проти України, встановлено наявність низки каналів матеріально-фінансового забезпечення терористичної

діяльності, що функціонують під прикриттям громадських об’єднань, гуманітарних організацій, так званих волонтерських ініціатив. У багатьох випадках ці структури використовуються як посередники у легалізації незаконних грошових потоків, зокрема шляхом купівлі обладнання, дронів, військової амуніції, засобів зв’язку, які в подальшому передаються бойовикам та диверсійно-розвідувальним групам на тимчасово окупованих територіях або безпосередньо в зону бойових дій [17].

Сучасна терористична діяльність дедалі частіше набуває рис неконвенційного протистояння, в якому фізичний акт насильства поступається або поєднується з психологічним впливом на масову свідомість. У цьому контексті інформаційно-психологічні операції (ІПсО) стають невід’ємною складовою терористичної стратегії, що має на меті зміну когнітивного сприйняття реальності, руйнування психологічної стійкості населення та формування соціальної дезорієнтації [1]. ІПсО в сучасному розумінні — це не просто розповсюдження дезінформації або ворожих наративів, а системний, технологічно організований комплекс дій, що спрямовані на формування бажаних моделей поведінки в суспільстві, створення страху, недовіри до влади, розгубленості й паніки.

Механізм дії ІПсО як інструмента терористичного впливу базується на багаторівневій структурі, де інформаційна атака виступає як спосіб створення у свідомості реципієнта відчуття загрози, невизначеності або зневіри. Зазвичай такі операції здійснюються одночасно в кількох медіасферах — соціальні мережі, телеканали, месенджери, публічні платформи. Ключовим об’єктом впливу є не лише інформаційний простір держави, але й психологічна цілісність індивідуума, зокрема його емоційне, ціннісне та поведінкове поле. Саме через це ІПсО можна визначити як форму «безконтактного терору», де вплив здійснюється без фізичного знищення, але з потенційно масштабними соціальними наслідками [23].

ІПсО, організовані або підтримувані терористичними структурами, мають чітко визначену мету — досягти психологічного паралічу ворожого середовища. Це досягається через низку методик: тиражування загроз (у тому числі фейкових

повідомлень про мінування, підготовку терактів, зникнення людей тощо); інспірування недовіри до державних органів (через дезінформаційні кампанії про нібито «зраду», «зливи» або «фальсифікації»); деструкція морального стану військовослужбовців та їхніх родин (через цільову пропаганду в Telegram, YouTube, TikTok); створення фрагментації суспільства шляхом розпалювання конфліктів на етнічному, мовному, релігійному чи політичному ґрунті [28].

Одним з найнебезпечніших напрямків ІПсО є використання терористами

Терористичні загрози, спрямовані на тилові, умовно безпечні регіони України, на сьогодні становлять один із ключових векторів гібридної війни, яку веде держава-агресор проти української державності [25]. Терористична активність у мирних регіонах не лише спрямована на створення відчуття небезпеки серед громадян, але й має стратегічну мету – дестабілізувати політичну ситуацію, підірвати довіру до органів влади, спровокувати паніку, порушити функціонування критичної інфраструктури та знизити стійкість суспільства до зовнішніх загроз.

Однією з основних форм такої діяльності є організація та координація диверсійно-терористичних груп, агентурно-розвідувальних мереж, а також здійснення кібератак і інформаційно-психологічного впливу, спрямованого на імітацію терористичних атак або їх підготовку. Впродовж 2022–2024 років правоохоронними органами України було задокументовано і нейтралізовано значну кількість терористичних інцидентів, спроб терактів, а також дій, що класифікуються як погроза їх вчинення, які мали місце у відносно спокійних регіонах – зокрема в Київській, Львівській, Вінницькій, Хмельницькій, Івано-Франківській, Полтавській та інших областях [28].

Характерною особливістю цих інцидентів є цілеспрямованість атак на стратегічно важливі об'єкти: залізничні вузли, енергетичні об'єкти, аеропорти, торгові центри, державні установи, освітні заклади. Такі об'єкти обираються з урахуванням їх високого символічного і функціонального навантаження у національній системі безпеки та соціальної стабільності. Дії терористів здебільшого координуються ззовні – через зашифровані месенджери, анонімні

криптоплатформи, системи прихованого фінансування, що ускладнює виявлення виконавців та замовників.

У відповідь на загострення загроз Служба безпеки України (СБУ) та інші силові структури активізували реалізацію комплексу превентивних заходів, серед яких — виявлення агентурних мереж, проведення контррозвідувальних операцій, нейтралізація вибухонебезпечних пристроїв, блокування каналів нелегального обігу зброї, вибухівки та хімічних реагентів. Водночас, спостерігається зростання ролі кіберкомпоненту в цих спробах дестабілізації: зловмисники використовують інформаційні платформи як засіб психологічного терору, поширюючи фейкові новини про мінування, нібито атаки безпілотників чи диверсії.

Іншим напрямом залишається активна деструктивна пропаганда, яка супроводжує або передує спробам терактів. Основний акцент у таких кампаніях робиться на деструкції психоемоційного стану громадян, підриві довіри до державних інституцій, створенні віртуальної дійсності, у якій Україна нібито не здатна забезпечити безпеку навіть у мирних регіонах [28]. У низці випадків були зафіксовані спроби розповсюдження відео- та фотоматеріалів, що інсценують теракти в українських містах, але насправді зняті в інших країнах або на окупованих територіях.

У результаті системної аналітичної роботи, до якої залучено не лише правоохоронні органи, але й аналітичні центри, дослідницькі інститути, IT-сектор, вдалося не лише локалізувати численні загрози, а й частково демонтрувати мережі, що координували такі дії. Значну увагу при цьому приділено профілюванню потенційних виконавців терористичних дій, зокрема осіб, які схильні до радикалізації, мають зв’язки з незаконними формуваннями або виявляють підвищену інтерес до зброї, вибухівки, підготовки до диверсійної діяльності [1].

Окремо варто відзначити факт активізації терористичних спроб у періоди національних свят, виборчих кампаній, публічних акцій, що свідчить про свідому прив'язку терористичної активності до символічно важливих подій. Мета такого підходу — максимальне інформаційне охоплення, створення

відчуття вразливості системи, трансляція у медіапростір сигналу про «всюдисущість загрози».

Особливо небезпечним викликом є спроби терористичних атак за участю неповнолітніх або осіб, які були під впливом ІПсО та маніпуляцій. Зокрема, виявлялися спроби залучення школярів до підготовки псевдомінувань або передачі інформації про охоронювані об'єкти. Такі дії свідчать про глибоку інфільтрацію терористичних наративів у соціальні та вікові групи, які раніше не розглядалися як уразливі.

Аналіз виявлених і попереджених спроб терактів дає підстави стверджувати, що системна дестабілізація тилових територій України є однією з головних довгострокових стратегій держави-агресора. Саме на цих територіях спостерігається активне формування осередків латентної небезпеки, які потребують постійного моніторингу, оцінювання ризиків, реалізації комплексних заходів безпеки. Механізм протидії має передбачати не лише реагування, але й постійне вивчення тенденцій розвитку терористичних практик, зокрема з урахуванням трансформацій форм і методів впливу на цивільне населення.

Феномен так званих «сплячих» осередків терористичних груп є однією з найнебезпечніших форм латентної загрози в сучасному безпековому середовищі. Їхня специфіка полягає у здатності зберігати прихований характер протягом тривалого часу, не виявляючи жодної активності, аж до моменту отримання інструкції до дії. Це робить традиційні механізми правоохоронного моніторингу переважно неефективними, а отже — зумовлює потребу в переосмисленні парадигми національної контртерористичної стратегії.

У сучасних умовах гібридної війни проти України, застосування таких осередків становить елемент асиметричного протиборства. Їхня функція — ускладнити виявлення джерела загрози, розосередити зусилля правоохоронної системи та паралізувати оперативне реагування на момент активації. Виявлення цих клітин ускладнюється завдяки високому рівню конспірації, адаптації до соціального середовища та використанню новітніх інформаційно-

комунікаційних технологій, включно з анонімними цифровими каналами координації, криптографією та кіберкампаніями дезінформаційного характеру.

Проблематика виявлення таких осередків пов’язана із їх здатністю мімікрувати під звичайні соціальні структури, громадські ініціативи або навіть релігійні об’єднання. Соціальна інтегрованість осіб, залучених до «сплячих» структур, мінімізує підозри з боку державних органів. Більше того, об'єктивні виклики — як-от велика кількість внутрішньо переміщених осіб, відкритість кордонів, інтенсивна міграція, зростання темпів радикалізації серед молоді — створюють ідеальне середовище для закріплення таких осередків у тилових регіонах.

Окремо варто акцентувати увагу на техніко-оперативному аспекті виявлення «сплячих» осередків. Класичні форми оперативної розвідки виявляються малоефективними, натомість на перший план виходять аналітико-прогностичні підходи — машинне навчання, аналіз великих даних (Big Data), побудова профілів ризику, когнітивне моделювання поведінки. У практиці багатьох держав — від Ізраїлю до США — домінує концепція превентивної безпеки (prevention-based intelligence), яка ґрунтується на постійному оновленні баз даних, поведінковому аналізі, інтеграції відомостей із різних систем моніторингу, включно з банками даних митниці, міграційної служби, телекомунікаційного нагляду.

Наявна в Україні система реагування на терористичні загрози потребує кардинального посилення превентивного сегменту. Як зазначається в дослідженні, значну роль у нейтралізації сплячих осередків відіграють аналітичні центри, дослідницькі структури, ІТ-сектор, які інтегруються в єдиний безпековий простір шляхом реалізації міжсекторальних програм обміну даними та проведення спільних експертиз. Зокрема, важливим є впровадження алгоритмів профілювання потенційно небезпечних осіб — за ознаками психологічної нестабільності, ідеологічної заангажованості, попереднього зв’язку з радикальними групами, підвищеного інтересу до зброї чи вибухових речовин.

Необхідно наголосити, що ключовим бар'єром у процесі нейтралізації таких осередків є правова колізійність та відсутність чіткої нормативної бази щодо профілактичних дій, які не мають під собою безпосереднього складу злочину. Відповідно, потребує розвитку інститут превентивної безпеки — не лише у вигляді змін до кримінального процесуального кодексу, а й через створення системи адміністративно-правового регулювання моніторингових та контррозвідувальних заходів. Правова модель має передбачати запобіжні механізми, які дозволяють зберегти баланс між захистом національної безпеки та дотриманням прав і свобод громадян.

Крім того, дієвим інструментом боротьби є інституціоналізація оперативного міжвідомчого хабу в межах сектору безпеки — на кшталт Національного аналітичного центру контртероризму, до складу якого повинні входити представники СБУ, МВС, НГУ, Державної прикордонної служби, а також спеціалізовані кіберпідрозділи. Завданням цього органу є забезпечення цілісності аналітичного поля, формування прогностичних моделей загроз, обмін оперативною інформацією в реальному часі та координація дій на випередження.

Ефективна протидія терористичним загрозам у сучасних умовах вимагає не лише наявності відповідного законодавчого механізму, підготовленого особового складу та технічного оснащення, але й чітко вибудуваної системи міжвідомчої взаємодії [25]. У національній системі безпеки України ключовими суб'єктами у сфері протидії тероризму виступають Служба безпеки України, Міністерство внутрішніх справ та підрозділи Національної гвардії України. Успішність реагування на терористичні виклики значною мірою залежить від здатності цих органів діяти як єдиний оперативно-інформаційний механізм, що забезпечує координацію на стратегічному, тактичному й оперативному рівнях.

Першочергове значення у цій системі належить Службі безпеки України, яка відповідно до Закону України «Про боротьбу з тероризмом» виконує функцію координатора зусиль усіх суб'єктів боротьби з тероризмом. Її роль не обмежується суто оперативною діяльністю [24]. Вона включає управлінсько-організаційне забезпечення, формування загальнодержавних концепцій протидії тероризму, моніторинг загроз національній безпеці, а також здійснення

аналітичного супроводу антитерористичних заходів. У цьому контексті СБУ фактично виконує функцію контррозвідувального та контртерористичного центру, який акумулює інформацію з різних джерел, систематизує її та перетворює на управлінські рішення, що мають критичне значення для національної безпеки.

Міністерство внутрішніх справ, у свою чергу, виконує розширену роль у системі превенції тероризму, зосереджуючи свою діяльність на виявленні ранніх ознак загроз, реалізації оперативно-розшукових заходів, профілактичній роботі в соціальних групах ризику, а також забезпеченні громадського порядку у періоди підвищеної терористичної загрози [1]. Зокрема, підрозділи Національної поліції, що підпорядковуються МВС, здійснюють патрулювання стратегічних об'єктів, супровід підозрілих осіб, реагування на повідомлення про замінування, ідентифікацію потенційних радикальних осередків. Ця функціональна роль особливо актуалізується у міських агломераціях, де ризик деструктивних дій терористичних груп є особливо високим у зв’язку з концентрацією критичної інфраструктури та масового скупчення населення.

Національна гвардія України в межах своїх функцій виконує завдання щодо безпосередньої підтримки сил безпеки у разі введення режиму контртерористичної операції, участі в заходах з локалізації та нейтралізації активних терористичних загроз, охорони особливо важливих державних об’єктів, здійснення евакуації населення та участі в операціях з припинення масових заворушень, які можуть мати терористичну мотивацію. Статус НГУ як військового формування з правоохоронними функціями дозволяє поєднувати оперативну маневреність, бойову підготовленість і правову інтегрованість у правове поле державного управління безпекою. Особливої уваги заслуговує взаємодія НГУ з СБУ при реалізації оперативних планів за умов введення режиму надзвичайного або воєнного стану [29].

Інституційна взаємодія цих органів ґрунтується на концепції міжвідомчої комплементарності, що передбачає не дублювання, а розмежування функцій із одночасною побудовою ефективного механізму інформаційного обміну. Практичне втілення цієї концепції здійснюється через систему

Антитерористичного центру при Службі безпеки України, що виконує функції координаційного штабу, у якому представлено усі ключові силові структури, включно з ДСНС, ДПСУ та органами військового управління. На етапі планування операцій АТЦ забезпечує інтеграцію сил і засобів усіх суб'єктів, їх логістичне забезпечення, юридичну легітимацію та стратегічну комунікацію з органами влади.

Період 2014–2024 рр. є знаковим для розуміння еволюції терористичних загроз в Україні, адже саме в ці роки відбулися фундаментальні трансформації як у внутрішньому безпековому середовищі держави, так і у зовнішньополітичному контексті. Анексія Автономної Республіки Крим, початок гібридної війни на сході України, багаторічна збройна агресія, а з 2022 року — повномасштабне вторгнення, змінили не лише конфігурацію національної безпеки, але й сутність тероризму як феномену в українському контексті [1].

2014 рік ознаменувався різкою радикалізацією загроз, які раніше мали спорадичний характер. Терористичні дії стали інструментом гібридної агресії — зокрема, у формі захоплення державних будівель, збройного спротиву легітимним органам влади, використання засобів масової інформації для створення паніки та дезорієнтації населення. Виник феномен некласичного тероризму — зокрема, з боку незаконних збройних формувань, які почали діяти в Донецькій і Луганській областях. За міжнародними критеріями, дії так званих «ДНР/ЛНР» мали всі ознаки терористичних організацій: використання насильства з метою залякування населення, прагнення впливати на прийняття державних рішень, наявність політичного мотиву, підтримка з боку іноземної держави.

Особливо показовим є етап 2014–2016 рр., коли терористичні загрози мали переважно «польовий» характер — тобто були пов'язані з фізичним насильством, актами саботажу, підривами військових і цивільних об'єктів. Цей період характеризується високим рівнем латентності терористичних актів, здійснюваних під прикриттям «повстанського» або «партизанського» руху. Основні загрози були зосереджені у зоні проведення АТО, проте зафіксовані

випадки терористичних актів у Харкові, Одесі, Києві [21]. Активізувалася діяльність диверсійно-розвідувальних груп, а також формувань, які здійснювали замахи на стратегічні об’єкти інфраструктури — мости, вокзали, об’єкти енергетики. Технологія терору набула нової форми — інформаційного супроводу з метою посилення психологічного ефекту серед населення.

Починаючи з 2017 року, спостерігалася відносна стабілізація ситуації. Завдяки активізації контррозвідувальної діяльності СБУ, впровадженню системи внутрішнього моніторингу та модернізації механізмів реагування, рівень терористичних актів істотно знизився. Однак структура загроз змінилася. Виникла тенденція до зростання кібертероризму, спрямованого на виведення з ладу об’єктів критичної інфраструктури — енергетичних систем, телекомунікацій, банківських ресурсів. Кібератака на енергомережу України в грудні 2015 року, яку міжнародна спільнота класифікувала як один із перших прикладів «інфраструктурного тероризму», засвідчила вразливість навіть модернізованих систем управління та контролю.

2018–2019 рр. позначилися зміщенням фокусу з активного фізичного терору до інформаційно-психологічних операцій (ІПсО). Посилення пропагандистської активності, дезінформаційні кампанії, кібератаки на ЗМІ, маніпуляція фактами із залученням соціальних мереж стали новою тактикою терористичних стратегій. Ці загрози мали значну інерцію, оскільки, на відміну від одноразових актів терору, спрямовані на довготривале формування атмосфери недовіри, соціального розколу, політичної дестабілізації. Терористичні загрози, таким чином, перестали бути суто фізичними й отримали виразну когнітивну складову.

2020 рік, позначений початком пандемії COVID-19, виявив нові вектори у формуванні терористичних ризиків. Під прикриттям надзвичайних обставин активізувались спроби зламів інформаційних систем охорони здоров’я, з’явилися повідомлення про фейкові замінування медичних установ, а також кіберкампанії із запуску фейкових повідомлень про зараження, карантинні бунти тощо. Саме в цей період почалося формування «м'яких» технологій терору — тобто маніпуляції масовою свідомістю через побоювання, які не мають

безпосередньої вибухової чи фізичної складової, але викликають ідентичний за ефектом суспільний резонанс і стресову дестабілізацію.

Після 24 лютого 2022 року розпочався абсолютно новий етап ескалації терористичних загроз в Україні, пов’язаний із повномасштабною військовою агресією. Тотальна мілітаризація терору — через удари по цивільному населенню, знищення об'єктів інфраструктури, обстріли шкіл, лікарень, ТЕЦ, вокзалів — продемонструвала цілеспрямовану стратегію державного терору. Слід акцентувати, що терористичні дії в цьому періоді набули системного, регулярного і стратегічного характеру, що дозволяє класифікувати їх як акти державного тероризму, за визначенням низки міжнародних правових актів та інтерпретацій міжнародного гуманітарного права [25].

У цьому ж контексті варто зазначити різке зростання ролі Національної гвардії, Служби безпеки України, кіберпідрозділів Міноборони та Держспецзв’язку в ідентифікації, попередженні та нейтралізації як фізичних, так і кібер- та інформаційних форм терору. Створення інтегрованих центрів безпеки, модернізація систем відеоспостереження, розгортання ситуаційних кімнат у регіонах та надання населенню інструментів для повідомлення про підозрілу активність — стали базисом нової парадигми превентивного реагування на терористичні ризики. При цьому безпекова стратегія України поступово трансформувалася з моделі реактивного реагування до системи прогностично-мережевого аналізу загроз, яка враховує динамічну зміну ризиків, у тому числі у форматі «сплячих» осередків, автономних кіберугруповань та гібридних суб’єктів насильства.

2023–2024 рр. продовжили тенденцію до еволюції форм терору. Зафіксовані численні приклади використання безпілотних літальних апаратів у містах поза межами лінії фронту, спроби підриву логістичних вузлів, атак на критичну інфраструктуру — зокрема, в галузі енергетики, водопостачання, транспорту. Посилилася взаємодія між державними та приватними структурами, зокрема в частині кібербезпеки, що стало відповіддю на зростання кібердиверсій. Інституційна модель національного реагування вийшла за межі суто силового

підходу і набула рис мультиінституційної інтеграції — із залученням фінансового сектору, телекомунікацій, енергетики, інфраструктури, ІТ-індустрії.

Зміна структури терористичних загроз у зазначений період має виразну фазову природу. Якщо у 2014–2016 рр. домінували фізичні загрози, пов'язані з активними діями терористичних груп, то в подальшому на перший план вийшли кібер-, інформаційні та когнітивні загрози, що вимагають нового методологічного підходу. Сучасний тероризм перестав бути винятково феноменом силового насильства і дедалі більше набуває форми структурного, мережевого та інституційного впливу — на інфраструктуру, моральний стан суспільства, політичну стабільність [25].

Зміна рівня терористичних загроз у період 2014–2024 рр. також відображає закономірності адаптації державного механізму реагування. Україна пройшла шлях від фрагментованої, некоординованої системи безпеки до функціонально зв'язаної моделі національного реагування. Запроваджено державні програми кіберзахисту, удосконалено антитерористичне законодавство, створено спеціалізовані підрозділи з виявлення та нейтралізації деструктивних впливів в інформаційному середовищі. Проте попри зростання інституційної зрілості, терористичні загрози продовжують бути непередбачуваними, особливо з огляду на глобальні ризики — поширення деструктивних ідеологій, посилення конкуренції держав за інформаційні впливи, дестабілізацію світової економіки та міграційні кризи.

Національна безпека України у XXI столітті перебуває під системним тиском багатовимірних загроз, з яких тероризм є не лише інструментом, а й відображенням загального середовища конфліктної невизначеності. Сучасний тероризм у контексті України не зводиться до класичних форм радикалізованого насильства, а існує як частина ширшого спектру гібридної війни, що поєднує інформаційні, економічні, ідеологічні, кібернетичні та воєнні компоненти. Саме тому осмислення актуальних викликів у цій сфері вимагає не лише аналізу поточних загроз, а й розуміння тих глибинних процесів, що формують нові ризики в контексті стратегічної трансформації безпекової архітектури.

Одним із ключових викликів є трансформація форми та структури терористичних дій. Якщо у 2014–2016 роках основну загрозу становили дії диверсійно-терористичних груп, які здійснювали акти фізичного насильства на територіях, близьких до зони бойових дій, то сучасна парадигма терористичної активності зміщується у площину когнітивного впливу, кіберзагроз та деструктивної дезінформації. Такі форми мають здатність проникати у глибокі рівні соціальної структури — інформаційний простір, системи освіти, внутрішньодержавний політичний дискурс — і тим самим підривати довіру до інститутів державної влади, викликати розчарування серед населення, формувати ілюзії поразки та капітуляціонізму [11]. У цьому контексті тероризм перестає бути лише насильницьким способом досягнення цілей і перетворюється на інструмент формування нового типу управлінської кризи — через делегітимацію, фрагментацію і послаблення внутрішнього суверенітету.

Особливе занепокоєння викликає інституційна асиметрія у системі реагування на терористичні загрози. Попри наявність законодавчо визначеного координуючого центру у вигляді Антитерористичного центру при СБУ, практика засвідчує фрагментарність міжвідомчої взаємодії, обмежену синхронізацію дій, дублювання повноважень та суперечності в юридичному тлумаченні деяких понять. В умовах динамічно змінюваного спектра загроз критичною є потреба в стандартизації оперативних процедур, уніфікації протоколів реагування, удосконаленні спільних баз даних і забезпеченні цифрової інтеграції між усіма суб’єктами безпеки. Без цього держава залишається вразливою до швидких, децентралізованих атак, які здійснюють як зовнішні суб’єкти, так і внутрішні радикалізовані елементи.

Терористичні ризики також ускладнюються через інфраструктурну вразливість держави, зокрема у сферах енергетики, транспорту, водопостачання, цифрової комунікації. Наявність застарілих елементів інженерної інфраструктури, недостатній рівень кіберзахисту, неуніфіковані системи реагування на техногенні інциденти, а також слабка інтеграція комерційного сектора до національної системи безпеки створюють передумови для високоефективних атак з низьким порогом витрат для агресора [5].

Найнебезпечнішим є поєднання кіберзагрози з фізичною деструкцією, коли підрив підстанції супроводжується атакою на центр обробки даних або провокаціями у медіапросторі. Ця синергія становить сучасну форму технологізованого терору, яка дедалі частіше застосовується державними й недержавними суб'єктами проти України.

Окремо слід підкреслити виклик радикалізації в соціальному середовищі, особливо серед молоді, ветеранів війни, представників маргіналізованих соціальних груп. У контексті соціально-економічної турбулентності, високої рівняння на нестабільність, зниження довіри до влади та впливу зовнішньої дезінформації, спостерігається зростання протестного потенціалу. Терористичні структури, особливо ті, що діють у форматі сплячих осередків або неформальних об'єднань, можуть використовувати цей потенціал як ґрунт для вербування, радикалізації, підготовки до автономних терористичних актів. Важливим аспектом цієї загрози є відсутність чіткої суб'єктності — радикалізований індивід, діючи самостійно (так званий lone wolf), може реалізувати акт терору без зовнішньої координації, що ускладнює виявлення, моніторинг та профілактику.

У цьому контексті актуалізується питання управління наративами. Сучасний тероризм дедалі більше використовує комунікативний простір як арену впливу. Успішність теракту часто залежить не від його фізичного масштабу, а від того, наскільки масово й глибоко він резонує в інформаційному полі. Саме тому одним із найважливіших інструментів протидії стає стратегічна комунікація — здатність держави контролювати, оформлювати, канонізувати і пояснювати події так, щоби не допустити паніки, утрати суб'єктності або легітимації терористичних актів у свідомості населення. Це вимагає високого рівня координації між державними інституціями, медіа, аналітичними центрами та міжнародними партнерами, що на сьогодні реалізовано фрагментарно і потребує інституційного оформлення.

Особливу загрозу становить також внутрішня ерозія правового поля, яка може виникнути внаслідок антидемократичної реакції на терористичні загрози. Упровадження надзвичайних повноважень, обмеження прав громадян,

розширення компетенцій силових структур без належного контролю створює ризик девальвації правового статусу особистості. У таких умовах боротьба з тероризмом може втратити свою легітимність і спровокувати нову хвилю радикалізації вже всередині самої системи. Баланс між безпекою та свободою — один із найвразливіших параметрів сучасної держави, що особливо проявляється під час довготривалого воєнного конфлікту. Лише наявність прозорої системи парламентського й громадського контролю, незалежного судочинства і відкритих механізмів скарг може запобігти ризику авторитарної деформації під прикриттям антитерористичної політики.

Нарешті, важливо враховувати адаптивність і динамічність самих терористичних структур. Вони не є статичними організаціями, а постійно змінюються, впроваджують нові технології, розширюють ідеологічну базу, переорієнтовуються на нові цільові аудиторії. Це вимагає від держави постійного переосмислення стратегій: оновлення законодавства, навчання кадрів, інвестицій у нові технології, міжнародного діалогу і гнучкої зміни тактик реагування. Інакше державна політика ризикує бути завжди на крок позаду — з усіма наслідками, які з цього випливають.

2.2. Напрями вдосконалення системи оцінки ризиків тероризму

Формування ефективної системи оцінки ризиків тероризму в умовах гібридної війни, високої технологічності терористичних загроз і динамічної трансформації соціально-політичного середовища є ключовим елементом національної безпеки України. На сучасному етапі державна безпекова політика повинна спиратися не лише на реактивні механізми реагування на вже реалізовані загрози, а й на здатність передбачити, спрогнозувати, сконцентрувати ресурси на запобіганні. Це можливо лише за умови наявності науково обґрунтованої, інституційно сталеної і технологічно адаптованої системи оцінювання терористичних ризиків, яка б враховувала не лише фактор події, а й динаміку змін у середовищі.

Одним із базових напрямів удосконалення системи є інституційне оновлення механізмів оцінки ризиків, зокрема через формалізацію міжвідомчих процедур. Сьогодні ключові державні органи, що відповідають за безпеку (СБУ, МВС, НГУ, ДПСУ, ДСНС), здійснюють оцінку ризиків у межах власної компетенції, без достатнього рівня інтеграції аналітичних платформ та методологічної єдності. Це призводить до ситуаційної розмитості оцінок і унеможливлює формування загальнодержавного профілю загроз. Для усунення цієї проблеми необхідне створення національного міжвідомчого аналітичного центру оцінки ризиків тероризму — органу, який акумулював би дані з усіх силових структур, здійснював би інтегральний аналіз загроз на основі багатофакторних моделей та формував би єдину матрицю оцінювання терористичних ризиків, розраховану як на національному, так і на регіональному рівнях.

Удосконалення системи також потребує впровадження стандартизованих методик оцінки загроз, які ґрунтуються на кількісних і якісних параметрах. Сьогодні Україна не має національної версії єдиної методології оцінки терористичних ризиків. Натомість використовуються адаптовані моделі, запозичені з міжнародного досвіду, переважно на рівні оперативних структур, без закріплення на нормативному рівні. Доцільним є прийняття національного стандарту (за аналогом ENISA, ISO 31000) оцінки ризиків, який би включав уніфіковані категорії загроз, визначення ймовірності, вразливості, потенційної шкоди, рівня захищеності об’єкта та прогнозованих наслідків. У рамках такої моделі особливу роль відіграє категоризація об’єктів за рівнем критичності (criticality index), що дозволяє диференціювати рівень захисту та уваги з боку відповідних органів.

Сучасна система оцінки ризиків має стати динамічною, а не статичною. Це означає, що методології аналізу повинні бути адаптовані до зміни параметрів середовища — геополітичної ситуації, технологічних зрушень, соціальної динаміки, нових акторів загроз. Для цього необхідне використання інструментів сценарного аналізу (scenario-based risk assessment), що дозволяє моделювати потенційні варіанти розвитку подій, ідентифікувати "тригери" активації

терористичних осередків, розраховувати реакцію системи безпеки та соціальні наслідки. У межах такої моделі ключовим аналітичним інструментом стає SWOT- і PESTLE-аналіз для визначення внутрішніх і зовнішніх факторів, що впливають на ризик появи терористичних загроз у конкретній галузі або регіоні.

Критично важливою передумовою є інтеграція аналітики великих даних (Big Data) та штучного інтелекту у процес оцінювання ризиків. Сучасний тероризм функціонує у кіберінфраструктурі, де класичні форми моніторингу — спостереження, агентурна розвідка — часто не дають результату або мають обмежений горизонт виявлення загроз. Використання алгоритмів машинного навчання, нейромережевих моделей, аналізу цифрових слідів (digital footprinting), когнітивного профілювання дозволяє здійснювати ідентифікацію потенційно небезпечних індикаторів — зокрема в онлайн-активності, транзакційній поведінці, комунікаційних шаблонах. Окремо варто вказати на потенціал OSINT (open-source intelligence), який дозволяє виявляти ранні ознаки радикалізації в публічному просторі без порушення приватності або втручання в персональні дані.

Іншим пріоритетним напрямом удосконалення системи оцінки ризиків тероризму є залучення приватного сектору — операторів інфраструктур, IT-компаній, телекомунікаційних провайдерів, логістичних підприємств, банків — до процесу аналітичного супроводу. У розвинених безпекових системах приватний сектор є не пасивним об’єктом загроз, а активним елементом попередження — шляхом участі у системах сповіщення, ідентифікації аномалій, забезпечення кіберзахисту, обміну індикаторами компрометації. В українських реаліях така взаємодія поки що не є системною. Необхідно на законодавчому рівні закріпити інструменти партнерства держави і бізнесу у сфері оцінки ризиків, включно з механізмами доступу до релевантних даних, спільного управління критичною інфраструктурою, навчанням персоналу та проведенням спільних тренувань.

Важливу роль у вдосконаленні системи відіграє створення карти ризиків (risk maps) — інструменту просторового аналізу, що дозволяє географічно візуалізувати рівень загроз за регіонами, категоріями об'єктів, типами загроз.

Такі карти повинні постійно оновлюватися і бути доступними для обмеженого кола суб'єктів безпеки та критичної інфраструктури. Вони мають включати не лише дані про потенційні цілі терористичних атак, а й інформацію про рівень соціальної напруги, індекси радикалізації, конфліктогенність, інфраструктурні вразливості. Саме карта ризиків є основою для розробки політик превенції, зонування сил і засобів безпеки, планування ресурсів, визначення обсягів фінансування превентивних заходів.

Оцінка ризиків тероризму має базуватися також на кроссекторальному підході, що передбачає включення у процес оцінки не лише силових органів, а й експертного середовища — академічних установ, think-tank-центрів, соціологічних служб, громадських організацій, правозахисних ініціатив. Завдяки цьому процес отримує мультиперспективність — з урахуванням культурних, соціальних, правових, психологічних чинників, що не завжди помітні в рамках класичної розвідки. Такий підхід посилює легітимність рішень, створює умови для довіри до аналітики, формує відкриту експертну дискусію та розширює спектр раннього попередження.

Не менш важливим напрямом є реформування системи навчання кадрів, залучених до процесу оцінки ризиків. Сьогодні система професійної підготовки фахівців у сфері безпеки переважно орієнтована на традиційні дисципліни: кримінологію, оперативну діяльність, право. Натомість оцінка ризиків потребує навичок із сфер математичного моделювання, кібербезпеки, аналізу даних, когнітивної психології, аналітичної логіки, системного мислення. Відповідно, слід створити спеціалізовані навчальні програми на базі закладів вищої освіти, профільних інститутів сектору безпеки та міжнародних платформ, які б готували аналітиків нового покоління — здатних працювати в умовах високої невизначеності та багатофакторності.

Удосконалення оцінки ризиків має також спиратися на підвищення правової адаптивності. Діючі нормативні акти часто передбачають жорсткі процедури реагування, але не забезпечують належної гнучкості у швидкозмінюваному середовищі ризиків. Необхідно оновити законодавство з урахуванням принципів гнучкого управління загрозами (adaptive governance),

запровадити інструменти превентивного ризик-менеджменту, створити правові умови для здійснення дій на випередження без порушення прав людини. Йдеться про легітимацію роботи з неперсоналізованими цифровими слідами, правове закріплення механізмів обміну ризиковими профілями, збереження інформації у хмарних системах тощо.

Таким чином, удосконалення системи оцінки ризиків тероризму не є технічним завданням вузького профілю, а передбачає системну трансформацію моделі національної безпеки — від реактивної до предиктивної, від фрагментарної до інтегрованої, від інтуїтивної до доказової. Тільки за умови поєднання інституційного оновлення, технологічної модернізації, міжсекторальної взаємодії та аналітичного прогнозування держава зможе забезпечити стійкість до терористичних загроз нового типу — багатовимірних, мережевих, технологізованих і когнітивних.

Висновки до розділу 2

У межах проведеного дослідження другого розділу магістерської роботи здійснено комплексний аналіз динаміки змін терористичних загроз в Україні у період 2014–2024 рр., із врахуванням їхніх геополітичних, соціально-політичних, інформаційних і безпекових параметрів. На основі систематизації емпіричних даних, відкритих джерел, звітів державних і міжнародних інституцій, а також опрацювання науково-аналітичної літератури, встановлено багатофакторний і трансформативний характер терористичних загроз, що суттєво ускладнює їх прогнозування та нейтралізацію в умовах гібридного конфлікту.

Визначено, що у перші роки збройної агресії проти України (2014–2016 рр.) тероризм набув форми диверсійно-силових дій, спрямованих на фізичне знищення об’єктів критичної інфраструктури, інституцій державної влади, а також залякування цивільного населення. З 2017 року простежується поступовий зсув акценту в бік інформаційно-психологічних, кібернетичних та когнітивних

форм терору, що спрямовані на створення атмосфери соціального страху, дестабілізацію політичного середовища та розмиття довіри до державних інституцій. У 2022–2024 рр. тероризм в Україні набуває масштабного характеру та систематичної реалізації у вигляді масованих ударів по цивільному населенню, енергетичній інфраструктурі, гуманітарних об’єктах, що дозволяє кваліфікувати дії Російської Федерації як форми державного тероризму, що супроводжує збройну агресію.

У процесі дослідження доведено, що терористичні загрози в Україні мають багатовекторну природу: поєднують фізичний терор, кібертероризм, інформаційно-психологічні операції, фінансування терористичних груп та маніпуляцію соціальним протестним середовищем. Кожен із вказаних векторів діє як окремий канал впливу, що ускладнює їхню ідентифікацію та підриває цілісність безпекової системи. З’ясовано, що системна вразливість полягає не лише в технічній чи організаційній недосконалості окремих елементів реагування, а в недостатній інтегрованості інституцій, фрагментації правових процедур і низькому рівні міжвідомчої аналітики.

Особливу увагу приділено аналізу трансформації структури терористичних загроз: від класичного організованого насильства — до асиметричних, децентралізованих, технологізованих атак, здійснених через анонімні кібермережі, автономних виконавців (так званих «одинаків»), цифрову пропаганду, симулятивні повідомлення про загрози (фейкові мінування тощо). Встановлено, що особливістю новітніх терористичних проявів є їхня здатність зливатися з повсякденним соціальним середовищем, уникати класичної розвідки і використовувати інструменти масової комунікації як канали терору.

Під час вивчення механізмів державної протидії було виявлено, що, попри створення низки спеціалізованих органів, наявні моделі реагування залишаються переважно реактивними, а система прогнозування ризиків не має належного ступеня аналітичної автономності, гнучкості та технологічної модернізації. Оцінено, що сучасні виклики терористичного характеру вимагають переорієнтації державної політики з акцентом на превентивні стратегії, багаторівневий моніторинг, кібернетичну адаптацію та побудову мережевих

структур ситуаційного аналізу. У зв’язку з цим сформульовано необхідність запровадження динамічної системи оцінки ризиків на основі міждисциплінарного підходу, що поєднує юридичні, безпекові, технологічні та соціокультурні компоненти.

Узагальнення здобутих результатів другого розділу дозволило виявити новітні характеристики терористичних загроз, визначити тенденції їх еволюції, встановити внутрішні слабкості безпекової архітектури України, а також обґрунтувати необхідність переходу до проактивної моделі протидії тероризму на основі аналітичної передбачуваності, інституційної узгодженості та адаптивного управління ризиками. Це створює логічне підґрунтя для розробки стратегічних напрямів удосконалення системи оцінки терористичних загроз, що стане предметом аналізу у наступному розділі.

ВИСНОВКИ

У результаті виконання першого завдання дослідження — розкрити змістовну сутність тероризму як суспільно небезпечного явища та здійснити класифікацію основних типів терористичних загроз за критеріями їх походження, форм реалізації та спрямованості — встановлено, що тероризм в умовах сучасного безпекового простору України є не лише кримінально-правовим феноменом, а багатовимірним соціально-політичним явищем, що проявляється у фізичному, інформаційному, ідеологічному, технологічному та психологічному вимірах. Узагальнено підходи до класифікації терористичних загроз з урахуванням їх генезису (внутрішні та зовнішні), форм реалізації (фізичні атаки, кібератаки, інформаційно-психологічний вплив), а також мотиваційної спрямованості (політична, релігійна, етнічна, ідеологічна). Доведено, що в умовах гібридної війни тероризм стає невід’ємною складовою ворожих дій проти держави, які часто маскуються під протестні чи інформаційні кампанії, але мають чітко виражену деструктивну мету.

Виконуючи друге завдання — дослідити сучасні наукові підходи до визначення терористичних ризиків та проаналізувати основні методи їх оцінки, що застосовуються у практиці протидії тероризму на національному та міжнародному рівнях — встановлено, що сучасна практика ризик-менеджменту

у сфері національної безпеки передбачає використання як якісних, так і кількісних методів. Проаналізовано такі інструменти, як матриці оцінювання ризиків (risk matrix), моделі сценарного прогнозування, методи SWOT-, PEST- та GAP-аналізу, а також інтегровані цифрові інструменти з використанням алгоритмів штучного інтелекту та аналізу великих даних. Зроблено висновок, що наявна методологічна база в Україні залишається фрагментарною і потребує адаптації до стандартів ISO 31000 та практик ЄС і ООН, з урахуванням специфіки національного безпекового ландшафту.

У рамках третього завдання — здійснити аналіз динаміки та специфіки розвитку терористичних загроз в Україні у період з 2014 по 2024 роки, з урахуванням гібридного характеру сучасної війни та новітніх форм деструктивної діяльності — проаналізовано багаторічну еволюцію форм терору в Україні: від організованих диверсій у зоні проведення АТО/ООС до масованих обстрілів цивільної інфраструктури та кібероперацій у період повномасштабної агресії. Виявлено тенденцію до переорієнтації противника на високотехнологічні, автономізовані форми впливу, що діють через децентралізовані платформи або симульовані соціальні конфлікти. Окремо досліджено форми так званого «державного тероризму», що реалізується Російською Федерацією як частина офіційної воєнної доктрини. Встановлено, що з 2022 року Україна стикається з постійними актами терору проти цивільного населення, об’єктів критичної інфраструктури, транспортної логістики, що потребує розробки довгострокової стратегії системної протидії.

Реалізуючи четверте завдання — визначити ключові проблеми, слабкі місця та системні недоліки у чинній моделі оцінки терористичних ризиків, що функціонує в українській безпековій системі — з’ясовано, що сучасна система залишається переважно реактивною, фрагментарною, недостатньо міжвідомчо інтегрованою. Виявлено відсутність єдиного аналітичного центру для агрегування інформації щодо терористичних загроз, низьку сумісність інформаційних платформ силових структур, обмежений доступ до інструментів передиктивного моделювання, слабку нормативну підтримку цифрових методів аналізу. Вказано на необхідність переходу від постфактум-контролю до системи

попереджувального аналізу з використанням інтегративного підходу, що поєднує юридичні, кібернетичні, соціальні та управлінські інструменти.

У процесі виконання п’ятого завдання — обґрунтувати науково-практичні напрями вдосконалення системи оцінки ризиків тероризму в Україні, включаючи пропозиції щодо правового, організаційного та аналітичного оновлення, з урахуванням світових стандартів і технологічного прогресу — сформульовано авторський концепт багаторівневої моделі оновлення оцінки ризиків. До нього входять: 1) розробка єдиного міжвідомчого стандарту аналізу загроз, 2) впровадження інтерактивної карти ризиків на основі статистично-логічних індикаторів, 3) посилення ролі штучного інтелекту у виявленні загроз, 4) закріплення на рівні закону інструментів превентивного моніторингу та кіберрозвідки, 5) залучення приватного сектору до національної системи оцінки ризиків, зокрема у сферах енергетики, IT, телекомунікацій. Обґрунтовано, що ефективна система має бути динамічною, прозорою, технічно гнучкою та правово захищеною.

Таким чином, усі поставлені завдання виконано повною мірою, а їх реалізація дозволила не лише поглибити теоретико-методологічну базу дослідження терористичних загроз, а й сформулювати практично значущі висновки для вдосконалення національної політики у сфері протидії тероризму.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бехруз Х.Н. Поняття війни у міжнародному праві: проблеми концептуалізації. *Юридичний науковий електронний журнал*. 2023. № 2. С. 558-561.
2. Варенья Н.М. Компетенція суб'єктів у протидії загрозам терористичного характеру. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція.* 2016. № 23. С. 177-180.
3. Грищук В.К. Тероризм: проблема поняття / *Тероризм і боротьба з ним. Аналітичні розробки, пропозиції наукових та практичних працівників: міжвідомчий науковий збірник* /під ред. А.І. Комарової, Ю.О. Землянського. Київ, 2020. Т. 19(1). С. 89–92.
4. Гуцало М. Організація протидії сучасному тероризму: навчальний посібник. Київ: Аратта, 2019. 263 с.
5. Демидова Л. М., Попович О. С. Кримінально-правова охорона національної безпеки України: терористичний акт : монографія. Харків: Право, 2021. 400 с.
6. Ємельянов В.П. Терористичний акт: загальне поняття, відмежування від суміжних злочинів та шляхи вдосконалення складу злочину. *Вісник Асоціації кримінального права України.* 2015. № 1(4). С. 233–244.
7. Жайворонок О. Причини і джерела ескалації інформаційного тероризму в Україні та світі. *Міжнародне право*. 2019. № 10. С. 218–223
8. Іванова Н. Г. Сутність мотиву особистості в теорії мотивації. *Вісник Національного університету оборони України.* 2021. № 3 (61), С. 20-27.

9. Кириченко О. В., Чорний О. М., Шамара О. В. Протидія терористичним актам в Україні: кримінально-правові та кримінологічні засади : монографія. Дніпро : Ліра, 2022. 181 с.
10. Конопельський В.Я. До питання про зарубіжний досвід організації протидії міжнародному тероризму. *Південноукраїнський правничий часопис.* 2019. № 3. С. 70–73.
11. Копанчук О.Є. Державний захист національних інтересів в інформаційній сфері України. *Актуальні проблеми державного управління*. 2020. № 1. С. 106-112.
12. Копанчук О.Є. Національні інтереси: теоретичний дискурс проблеми. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*. 2020. Вип. 1(10). С. 45-51.
13. Кримінальний кодекс україни. Відомості Верховної Ради України, 2001, № 25-26, ст.131
14. Кудінов С. С. Міжнародний досвід протидії тероризму та його значення для України. *Вчені записки ТНУ імені В.І. Вернадського*. 2019. № 1. С. 117-123.
15. Кудінов С. С. Правова політика з формування антитерористичної компетентності в Україні : моногр. Одеса : ФОП Букаєв Вадим Вікторович, 2019. 268 с.
16. Кудінов С. С., Рижов І. М., Романов М. С. Основи терорології : навч. посіб. Острог : Національний університет «Острозька академія», 2019. 200 с.
17. Кудінов С.С. Державний тероризм – визначення та характеристика. *Інформація і право.* № 2(41)/2022. С. 78-84.
18. Маделик С.М. Історичні витоки та еволюція тероризму. *Проблеми міжнародних відносин: Зб. наук. пр.* 2010. Вип. 1. С. 327–339.
19. Морозов О. М. Тероризм. Системна війна. Державна безпека. *Героїзм і психофізіологія*. Київ, 2019. 64 с
20. Організаційно-правові основи запобігання тероризму: підручник / Ю.О. Лісіцина, І.Р. Серкевич, Г.З. Яремко та ін. / за заг. ред. В.В. Луцика. Львів: ЛьвДУВС, 2020. 432 с.

21. Орловський Р. С., Валовина М. А. Суспільно небезпечні наслідки злочину. *Науковий вісник Херсонського державного університету. Серія: Юридичні науки*. 2017. Вип. 6, т. 3. С. 76–80
22. Павленко В. Вдосконалення кримінальної відповідальності за злочини, пов'язані з тероризмом. *Підприємництво, господарство і право*. 2018. № 11. С. 200–204.
23. Попович О.С. Терористичний акт: поняття, склад злочину, кваліфікація: автореф. дис. ... канд. юрид. наук. Харків, 2019. 20 с
24. Про боротьбу з тероризмом: Закон України від 20.03.03 р. № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення: 15.09.2024).
25. Протидія проявам тероризму та колабораціонізму в умовах війни: стан та перспективи*: матеріали Всеукраїнського круглого столу (м. Кропивницький, 24 листопада 2023 року).* Донецький державний університет внутрішніх справ. Кропивницький, 2023. 108с.
26. Протидія терористичним актам у міському середовищі: *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. 396 с.
27. Рижов І. М., Кудінов С. С., Івахненко О. А. Основи антитерористичної безпеки соціальних систем: монографія. Київ: Кафедра, 2017. 212 с.
28. Рубащенко М.А., Мовчан Р.О. Кримінальні правопорушення проти державної безпеки в проєкті нового Кримінального кодексу України. *Аналітичнопорівняльне правознавство*. 2023. №3. С. 328–341.
29. Семенченко А. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України: монографія. Київ: НАДУ, 2008. 428 с.
30. Серкевич І.Р. Кримінологічні детермінанти та кримінально-правова протидія тероризму: автореф. дис. … канд. юрид. наук. Львів: ЛьвДУВС, 2015. 215 с.

31. Ситник Г.П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади). Київ : НАДУ, 2011. 730 с.
32. Тацій В. Я. Обєкт і предмет злочину в кримінальному праві. Харків : Право, 2016. 256 с.
33. Теоретичні основи національної безпеки України : навч. посіб. для студ. вищ. навч. закладів / О. Дзьобань, О. Соснін. Київ: Освіта України, 2009. 384 с.
34. Тероризм: кримінологічна детермінація і кримінально-правова протидія: монографія / В.В. Середа, І.Р. Серкевич; за заг. ред. В.С. Канціра. Львів: ЛьвДУВС, 2016. 188 с.
35. Тихий В. П. Безпека людини: поняття, правове забезпечення, значення, види. *Вісник Національної академії правових наук України*. 2016. № 2 (85). С. 31-46.
36. Тютюгін В. І., Рубащенко М. А. Кримінальне право України. Загальна частина : посіб. для підгот. до заліків та іспитів. Харків : Право, 2024. 250 с.
37. Француз А.Й., Сніцаренко К.О. Класифікація тероризму в світі. Способи та елементи класифікації. *Legal Bulletin*. 2024. (№14), 161–164
38. Хаваліц О. В. Використання криміналістично значущих ознак під час виявлення та розслідування злочинів терористичного характеру. Науковий вісник Херсонського державного університету. 2016. С. 114–118.
39. Ahmad N., Majeed M.T. Does Political Globalisation Impede Terrorism? ARegional Perspective. *The Pakistan Development Review*. 2016. P. 409–423.
40. Alsawalqa R.O. Dialectical Relationship Between Terrorism and Human Security: A Sociological Approach. *Utopía y Praxis Latinoamericana*. 2021. Vol. 26. no. Esp.1. P. 275–285.
41. Atran S. Psychology of Transnational Terrorism and Extreme Political Conflict. *Annual Review of Psychology*. 2021. Vol. 72: P. 471–501
42. Erlenbusch, V. Terrorism and revolutionary violence: the emergence of terrorism in the French Revolution. *Critical Studies on Terrorism*. 2015. № 8(2). P. 193–210.

43. Forst B. A Brief History of Terrorism. In: Terrorism, Crime, and Public Policy. Cambridge University Press; 2008. P. 43–72.
44. Tymoshenko V.I., Maksymov S.I., Makarenko L.O., Kravchenko O.S., Kravchenko S.S. Threats to human rights in a globalized world. *Amazonia Investiga*. 2021. Vol. 10. № 39. P. 9–15