Наукове забезпечення як системоутворювальна основа антитерористичної безпеки України

Scientific Support as a System-Forming Foundation of Counter-Terrorism Security in Ukraine

Григорій Галаган
Corresponding author: аспірант, e-mail: medmil.ua@gmail.com, ORCID ID: https://orcid.org/0009-0004-9124-930X

Ігор Рижов
доктор юридичних наук, професор, заслужений юрист України, професор кафедри, e-mail: ryshow@gmail.com, ORCID ID: https://orcid.org/0000-0001-8009-5895

Петро Ящук
аспірант, e-mail: medmil.ua@gmail.com, ORCID ID: https://orcid.org/0009-0009-9367-0604

[A] Національна академія Служби безпеки України, м. Київ, Україна

Hryhorii Halahan
Corresponding author: PhD student, e-mail: medmil.ua@gmail.com, ORCID ID: https://orcid.org/0009-0004-9124-930X

Igor Ryzhov
Dr of Law, Professor, Honored Lawyer of Ukraine, Professor of the Department, e-mail: ryshow@gmail.com, ORCID ID: https://orcid.org/0000-0001-8009-5895

Petro Yashchuk
PhD student, e-mail: medmil.ua@gmail.com, ORCID ID: https://orcid.org/0009-0009-9367-0604

[A] National Academy of the Security Service of Ukraine, Kyiv, Ukraine

Received: September 14, 2026 | Revised: September 24, 2026 | Accepted: October 31, 2026

УДК 351.746.1:001.89:323.28:351.86(477)

DOI: https://doi.org/10.33445/sds.2026.16.5.1

Мета роботи. Обґрунтувати науку як системоутворювальну основу антитерористичної безпеки України, розкрити основні виміри її функціонування та сформувати засади інституціоналізації наукового забезпечення боротьби з тероризмом.

Метод дослідження. Застосовано системний, людиноцентричний, порівняльно-правовий і функціональний підходи, контент-аналіз нормативних та міжнародних документів, тематичний синтез наукових публікацій, концептуальне моделювання та метод аналітичної матриці.

Результати дослідження. Сформульовано авторське визначення наукового забезпечення та розмежовано його з науковим супроводом, інноваційною діяльністю, трансфером результатів і оцінюванням ефективності. Визначено сім функцій науки та розроблено цикл перетворення операційних даних на апробоване рішення. Обґрунтовано науково-інноваційний контур, вітальний критерій ефективності та диференційований доступ до захищених даних. Виявлено процесуальну прогалину в інституціоналізації постійної дослідницької функції та запропоновано трирівневу модель стратегічної координації, виконавчого науково-аналітичного супроводу й спеціалізованої освітньо-дослідної діяльності.

Теоретична цінність дослідження. Концептуалізовано вітальну складову антитерористичної безпеки та обґрунтовано функціональний, а не адміністративний зміст первинності науки.

Практична цінність дослідження. Результати можуть бути використані для визначення дослідницьких пріоритетів, перевірки інновацій, розвитку професійних компетентностей, організації контрольованого доступу до знеособлених даних та оцінювання впливу рішень на життя людини.

Оригінальність дослідження. Оригінальність полягає в поєднанні випереджального вироблення знань, інноваційного циклу, інституційного зворотного зв'язку та вітального критерію результативності в межах єдиної концептуальної конструкції.

Обмеження / напрями подальших досліджень. Запропоновані моделі потребують експертної перевірки, операціоналізації показників і пілотної апробації на окремих дослідницьких завданнях.

Тип статті. теоретико-концептуальна.

Purpose. To substantiate science as a system-forming foundation of counter-terrorism security in Ukraine, elucidate the principal dimensions of its functioning, and establish the basis for institutionalising scientific support for counter-terrorism.

Method. The study employs systemic, human-centred, comparative legal, and functional approaches, together with content analysis of regulatory and international documents, thematic synthesis of scholarly publications, conceptual modelling, and the analytical matrix method.

Results. The study formulates an original definition of scientific support and distinguishes it from scientific advisory support, innovation activities, research output transfer, and effectiveness evaluation. Seven functions of science are identified, and a cycle for transforming operational data into a tested solution is developed. The study substantiates a scientific innovation framework, a vital criterion of effectiveness, and differentiated access to protected data. A procedural gap in the institutionalisation of a permanent research function is identified, and a three-tier model encompassing strategic coordination, executive-level scientific and analytical support, and specialised educational and research activities is proposed.

Theoretical Implications. The vital dimension of counter-terrorism security is conceptualised, and the primacy of science is substantiated as functional rather than administrative in nature.

Practical Implications. The findings can be used to establish research priorities, test innovations, develop professional competencies, organise controlled access to anonymised data, and assess the impact of decisions on human life.

Originality/value. The originality of the study lies in integrating anticipatory knowledge generation, the innovation cycle, institutional feedback, and a vital criterion of effectiveness within a unified conceptual framework.

Limitations/future research. The proposed models require expert evaluation, operationalisation of relevant indicators, and pilot testing within selected research tasks.

Article type. theoretical and conceptual.

Ключові слова: державна безпека; тероризм; наукове забезпечення боротьби з тероризмом; людиноцентрична парадигма; вітальна безпека; прогнозування терористичних загроз; науково-інноваційний контур.

Keywords: State Security; Terrorism; Scientific Support for Counter-Terrorism; Human-Centred Paradigm; Vital Security; Terrorist Threat Forecasting; Scientific Innovation Framework.

Вступ

Сучасний тероризм є динамічним і технологічно адаптивним явищем, трансформація якого прискорюється під впливом воєнно-політичних конфліктів, цифровізації, глобалізації інформаційного простору та поширення технологій подвійного призначення. Терористичні організації, автономні осередки й окремі радикалізовані особи використовують соціальні мережі, зашифровані комунікації, синтетичні медіа, кіберінструменти та нові способи фінансування. Унаслідок цього терористична загроза виходить за межі фізичного насильства й одночасно охоплює інформаційний, когнітивний, кібернетичний, технологічний, фінансовий і соціально-психологічний простори [9; 13].

Зміна характеру терористичних загроз вимагає переходу від переважно реактивної моделі протидії до їх випереджального пізнання, прогнозування та запобігання. Визначальна роль науки у здійсненні такого переходу полягає у встановленні причинно-наслідкових зв'язків, побудові сценаріїв, оцінюванні ризиків, розробленні й апробації технологічних та організаційних рішень, а також перевірці їх фактичної результативності. Необхідність виконання зазначеного комплексу завдань виключає зведення ролі науки в боротьбі з тероризмом до допоміжного експертного супроводу вже ухвалених рішень. Наука має виконувати системоутворювальні, випереджальні, методологічні й доказові функції, поєднуючи в єдиний безперервний цикл виявлення практичної потреби, формування дослідницького завдання, одержання нового знання, упровадження обґрунтованого рішення та оцінювання наслідків його реалізації.

Сучасні дослідження розкривають окремі складові цього складного явища. Встановлено багатофакторний характер когнітивної та поведінкової радикалізації, що унеможливлює її надійне прогнозування за однією ознакою або універсальним профілем [38; 8]. Систематичні огляди програм запобігання насильницькому екстремізму водночас свідчать про неоднорідність індикаторів, обмеженість порівнянних емпіричних даних і недостатню перевірку довгострокового ефекту втручання [20; 19]. У цифровому вимірі дослідники аналізують зміну ролі приватних платформ, розвиток кіберризиків і подвійне призначення штучного інтелекту, наголошуючи на необхідності прозорості, валідації та людського контролю [7; 16; 34]. Дослідження стійкості критичної інфраструктури зміщують увагу від захисту окремого об'єкта до збереження функцій взаємозалежних систем та недопущення каскадних наслідків [24; 15; 35].

Значний обсяг накопичених наукових напрацювань ще не забезпечив цілісності дослідницького поля, яке продовжує характеризуватися тематичною та методологічною фрагментарністю. Радикалізація, цифрове середовище, штучний інтелект, критична інфраструктура, кризове реагування, професійна підготовка та права людини часто досліджуються як відносно автономні напрями. Зберігається також загальна методологічна проблема антитерористичних досліджень, що охоплює дефіцит первинних даних, обмежену відтворюваність результатів і недостатню кількість методологічно обґрунтованих оцінок ефективності контртерористичних заходів [29; 19]. Сукупний вплив зазначених методологічних обмежень призводить до того, що кількісне зростання наукових публікацій не завжди забезпечує формування цілісної та надійної доказової основи державної антитерористичної політики.

Особливої ваги набуває людиноцентрична спрямованість боротьби з тероризмом. Її кінцевим результатом має бути не лише нейтралізація суб'єкта загрози або забезпечення формальної захищеності об'єкта, а насамперед збереження життя, здоров'я, гідності та функціональної спроможності людини. Концепція вітальної безпеки орієнтує дослідження на захист життєвого потенціалу людини та суспільства в умовах складних взаємопов'язаних загроз [26; 27]. Її застосування до антитерористичної сфери дає підстави розглядати вітальну

складову антитерористичної безпеки як інтегрувальний критерій визначення пріоритетів, добору засобів і оцінювання практичної результативності.

Міжнародні підходи поєднують превенцію, розвиток державних спроможностей, технологічну адаптацію та забезпечення прав людини, але не встановлюють універсального національного механізму інституціоналізації наукового забезпечення.

Ключова суперечність сучасної боротьби з тероризмом полягає в тому, що терористичні суб'єкти швидко адаптують організаційні моделі, технології та способи впливу, тоді як державна система вимушена діяти в межах нормативно визначених процедур, відомчого розподілу компетенції та обмежених циклів оновлення спроможностей. Доступність цифрових платформ, зашифрованих комунікацій, безпілотних систем, технологій штучного інтелекту й інструментів кіберзлочинності скорочує час між виникненням нової можливості та її протиправним використанням. У результаті переважно реактивна модель, зорієнтована на виявлення підготовки, припинення терористичного акту та мінімізацію вже заподіяних наслідків, не гарантує необхідного інтелектуального й технологічного випередження.

Практичні підрозділи накопичують значні масиви відомостей про індикатори загроз, поведінку суб'єктів, способи підготовки, результати оперативних заходів, навчань і кризового реагування. Однак ці дані мають різне призначення, рівень повноти, формат і режим доступу. За відсутності постійного механізму їх наукового опрацювання операційний досвід не завжди трансформується у відтворюване знання, а практична потреба — у належно сформульоване наукове завдання. Виникає розрив між даними, дослідженням і рішенням: відомості залишаються в межах окремих суб'єктів; результати наукових праць не проходять системної апробації; ефект упроваджених заходів не завжди вимірюється за наперед визначеними критеріями.

Однією з причин виявленого розриву є обмежений доступ дослідників до належно знеособлених операційних даних. Відповідні обмеження об'єктивно зумовлені необхідністю охорони державної таємниці, захисту джерел інформації й персональних даних, а також нерозголошення методів і тактики діяльності уповноважених органів. Збереження необхідних режимних обмежень за повної відсутності регламентованого дослідницького доступу звужує можливості формувати репрезентативні вибірки, незалежно перевіряти наукові припущення, виявляти системні помилки та встановлювати причинний зв'язок між застосованим заходом і фактичною зміною рівня ризику. Наукова література підтверджує, що оцінювання програм запобігання радикалізації досі характеризується неоднорідністю методик, дефіцитом порівнянних даних і недостатньою перевіркою довгострокових наслідків [20; 19]. Розв'язання виявленої суперечності потребує не скасування режимних обмежень, а створення диференційованого, контрольованого та підзвітного механізму доступу дослідників до знеособлених наборів операційних даних.

Окремим проявом проблеми є використання штучного інтелекту. Терористичні суб'єкти можуть застосовувати генеративні системи для масштабування пропаганди, персоналізації вербувальних повідомлень, створення синтетичного контенту та підтримки кібероперацій. Водночас аналітичні інструменти ШІ здатні допомагати уповноваженим органам опрацьовувати великі масиви інформації, виявляти аномалії й моделювати сценарії [16; 30]. Подвійне призначення технології унеможливлює її оцінювання лише за функціональними можливостями. До впровадження потрібні наукова валідація на релевантних даних, визначення показників точності, перевірка стійкості моделі, пояснюваність результатів, людський контроль і процедура відповідальності за помилкове рішення. Інакше алгоритмічна помилка може призвести як до пропуску реальної загрози, так і до непропорційного втручання у права людини [34].

Нормативне регулювання України визначає суб'єктів боротьби з тероризмом, рівні терористичних загроз, засади міжвідомчої взаємодії, реагування та мінімізації наслідків.

Концепція боротьби з тероризмом в Україні 2026 року орієнтує державну систему на розвиток аналітичних, прогностичних, технологічних і кадрових спроможностей [6]. Проте в механізмі функціонування єдиної державної системи, затвердженому постановою Кабінету Міністрів України № 92, окремого постійного науково-дослідного сегмента прямо не передбачено [3]. Відсутність у зазначеному механізмі постійного науково-дослідного сегмента означає, що на нормативному рівні не сформовано завершеного циклу, який охоплював би визначення пріоритетів досліджень, формування наукових завдань, захищену роботу з даними, міждисциплінарне розроблення рішень, апробацію інновацій, проведення науково-технічної експертизи та оцінювання результативності впроваджених розробок. Наявність окремих досліджень, освітніх програм і експертних ініціатив не усуває виявленої прогалини, оскільки відповідні елементи не об'єднані постійним механізмом постановки завдань, практичного впровадження результатів і зворотного зв'язку з антитерористичною практикою.

Другою складовою досліджуваної проблеми є недостатня інституціоналізація людиноцентричного, або вітального, критерію антитерористичної безпеки. Кількість проведених заходів, виявлених загроз, припинених терористичних актів чи обладнаних засобами захисту об'єктів характеризує активність і окремі результати функціонування системи, але не забезпечує вичерпного оцінювання її суспільної ефективності. Визначальним має бути те, наскільки ухвалені рішення запобігають загибелі й травмуванню людей, забезпечують збереження їхнього здоров'я, гідності та життєвого потенціалу, а також безперервний доступ до життєво необхідних функцій і послуг. Концепція вітальної безпеки створює теоретичну основу для відповідного зміщення пріоритетів [26; 27]. Наявність відповідного теоретичного підґрунтя ще не супроводжується формуванням цілісного науково-практичного механізму, який визначав би структуру вітальної складової антитерористичної безпеки, її вимірювані показники та порядок їх урахування під час планування, експертизи й оцінювання антитерористичних заходів.

Сукупність виявлених нормативних, інституційних і методологічних розривів дає підстави сформулювати центральну дослідницьку проблему як відсутність цілісного інституціоналізованого циклу, у межах якого операційні дані та практичні потреби перетворювалися б на науково обґрунтовані завдання, результати досліджень — на апробовані антитерористичні рішення, а наслідки практичного застосування відповідних рішень — на доказову основу для коригування діяльності уповноважених суб'єктів і державної політики. Розв'язання визначеної проблеми потребує утвердження науки як системоутворювальної та випереджальної основи боротьби з тероризмом, нормативного й організаційного забезпечення постійної взаємодії між наукою та практикою, а також упровадження вітального критерію, за яким збереження життя, здоров'я і функціональної спроможності людини становить визначальний показник результативності антитерористичної діяльності.

Актуальність дослідження зумовлена суперечністю між швидкістю технологічної та організаційної трансформації тероризму і спроможністю державної системи своєчасно пізнавати, прогнозувати й випереджати відповідні загрози. Для України ця проблема посилюється поєднанням терористичних, диверсійних, кібернетичних та інформаційно-психологічних методів у контексті триваючої збройної агресії. За відсутності цілісного наукового контуру практичний досвід може не перетворюватися на перевірене знання, інновації — упроваджуватися без належної валідації, а результативність заходів — визначатися без достатнього врахування їх впливу на життя і здоров'я людини.

Метою статті є теоретичне обґрунтування системоутворювальної та випереджальної ролі науки в забезпеченні антитерористичної безпеки, а також розроблення концептуальних засад інституціоналізації наукового забезпечення загальнодержавної системи боротьби з тероризмом в Україні.

Для досягнення мети поставлено такі дослідницькі завдання: визначити зміст і функції наукового забезпечення боротьби з тероризмом; установити ключові розриви між накопиченням операційних даних, проведенням досліджень та упровадженням практичних рішень; розкрити сутність людиноцентричної парадигми й вітальної складової антитерористичної безпеки; оцінити нормативне та інституційне закріплення науково-дослідної функції; сформувати авторські пропозиції щодо постійної взаємодії між координаційними органами, оперативними підрозділами, закладами освіти та науковими установами.

Наукова новизна полягає в обґрунтуванні науки не як допоміжного ресурсу, а як системоутворювальної, випереджальної та доказової основи антитерористичної діяльності; концептуалізації вітальної складової антитерористичної безпеки як людиноцентричного напряму, у межах якого збереження життя і життєвого потенціалу людини становить визначальний критерій ефективності; формуванні циклічної моделі перетворення операційних даних на наукове знання, знання — на апробоване рішення, а результатів застосування — на підставу для коригування практики й державної політики. Подальшого розвитку набувають концептуальні засади інституціоналізації постійного наукового забезпечення боротьби з тероризмом в Україні.

Огляд літератури

Наукове осмислення тероризму характеризується значною міждисциплінарністю поряд із фрагментарністю дослідницького поля. Schuurman [29], узагальнюючи розвиток досліджень тероризму у 2007–2016 роках, звернув увагу на обмеженість первинних емпіричних даних, повторюваність окремих тем і недостатню прозорість застосовуваних методів. Значно раніше Lum et al. [18] встановили, що серед великого масиву публікацій лише незначна частина містила оцінки результативності контртерористичних заходів, які відповідали належним методологічним критеріям. Пізніші дослідження засвідчують, що відповідну методологічну проблему повністю не подолано. Madriaza et al. [19] за результатами систематичного огляду програм запобігання насильницькому екстремізму виявили недостатню якість дизайну багатьох оцінювань, неоднорідність індикаторів і складність установлення причинного зв’язку між здійсненим втручанням та одержаним результатом. Збереження виявлених методологічних обмежень упродовж тривалого періоду свідчить, що кількісне зростання публікацій саме по собі не забезпечує формування надійної доказової бази державної політики. Необхідними передумовами її створення залишаються доступ до валідних даних, застосування відтворюваних методик і порівнянних критеріїв, а також перевірка практичної ефективності антитерористичних заходів.

Зіставлення цих праць виявляє фундаментальну суперечність антитерористичних досліджень: найбільш цінні для науки відомості часто містяться в матеріалах з обмеженим доступом, тоді як відкриті публікації нерідко ґрунтуються на повідомленнях медіа, судових рішеннях або вторинних базах даних. Обмеженість доступу зумовлена необхідністю охорони державної таємниці, захисту джерел інформації та нерозголошення методів роботи, однак звужує можливості незалежної перевірки наукових висновків. Необхідність узгодження захисту чутливої інформації з вимогами наукової відтворюваності визначає регламентований доступ до знеособлених операційних даних як перспективний напрям розвитку антитерористичних досліджень. Запровадження нормативно врегульованого й диференційованого механізму доступу до відповідних даних створило б умови для формування репрезентативних вибірок, перевірки прогностичних інструментів, виявлення системних помилок та відмежування фактичного ефекту антитерористичного заходу від формальних показників організаційної звітності.

Окремий масив праць присвячений причинам і механізмам радикалізації. Wolfowicz et al. [38] систематизували фактори когнітивної та поведінкової радикалізації й довели, що їх

прогностична значущість залежить від контексту, рівня аналізу та форми радикалізаційного результату. Clemmow et al. [8] розвинули профільний підхід, показавши, що вразливість виникає внаслідок конфігурації факторів ризику і захисних чинників, а не дії однієї ознаки. Ці висновки мають принципове значення для антитерористичного прогнозування: науково необґрунтоване профілювання може продукувати хибнопозитивні оцінки, стигматизацію та непропорційне втручання у права людини. Mazerolle et al. [20], досліджуючи міжвідомчі програми за участю поліції, встановили обмеженість доказів їх впливу на зниження радикалізації до насильства. Сукупно ці праці підтверджують, що превенція потребує не універсальних переліків "небезпечних ознак", а багаторівневих моделей, локальної валідації та постійного оцінювання наслідків втручання.

Цифровізація змінила не лише засоби терористичної діяльності, а й структуру суб'єктів, залучених до протидії їй. Borelli [7] дослідила трансформацію соціальних медіакорпорацій у фактичних учасників контртерористичного регулювання, які через модерацію, автоматизоване виявлення та обмеження поширення контенту впливають на реалізацію безпекової політики. Така участь розширює технологічні можливості протидії, але водночас порушує питання прозорості алгоритмів, підзвітності приватних платформ і співвідношення безпеки зі свободою вираження поглядів. Cremer et al. [9] у систематичному огляді кіберризиків акцентували на неоднорідності, неповноті та недостатній доступності даних, що обмежує побудову надійних моделей. Leszczyna [17] показав, що методи оцінювання кібербезпеки істотно відрізняються за призначенням, ресурсомісткістю та практичною застосовністю. Farber [13] виявив поступове зближення окремих інструментів кіберзлочинців і терористів, зокрема використання цифрової інфраструктури, криптоактивів та анонімізованих середовищ, але застеріг від автоматичного ототожнення цих явищ. Це вимагає точного наукового розмежування мотивів, суб'єктів і наслідків відповідної діяльності.

У новітніх дослідженнях особливу увагу приділено штучному інтелекту. Lakomy [16] розглянув генеративні чатботи й системи створення зображень як потенційні засоби масштабування пропаганди, адаптації повідомлень і виробництва терористичного контенту. Ganaie [14] пов'язав алгоритмічні механізми цифрових платформ із радикалізацією, вербуванням і поширенням насильницького екстремізму, одночасно вказавши на можливості прогнозної аналітики для раннього виявлення загроз. Syllaidopoulos et al. [30] систематизували напрями застосування ШІ у контртерористичній діяльності та кібербезпеці, виокремивши аналіз даних, розпізнавання закономірностей і підтримку рішень поряд з етичними ризиками. Wall [34] обґрунтував необхідність оцінювати використання ШІ як цілісну соціотехнічну систему, у якій якість даних, точність моделі, людський контроль і наслідки помилки є взаємопов'язаними. Спільним для цих досліджень є визнання подвійного призначення ШІ; недостатньо розробленими залишаються стандарти його валідації саме для антитерористичних завдань, межі автоматизації та процедури відповідальності за помилкові рішення.

Вагомий напрям становлять дослідження стійкості критичної інфраструктури. Mottahedi et al. [21] узагальнили системні підходи до її стійкості й показали необхідність поєднання технічних, організаційних і управлінських складових. Sathurshan et al. [28] проаналізували рамки вимірювання стійкості та встановили відсутність універсального набору показників, придатного для всіх секторів і типів загроз. Osei-Kyei et al. [24] систематизували індикатори критичної інфраструктури, наголосивши на потребі узгодження критеріїв готовності, поглинання впливу, відновлення й адаптації. Wells et al. [37] показали складність моделювання інфраструктури за умов комбінованих загроз, коли наслідки виникають через взаємодію кількох факторів. Ji et al. [15] узагальнили обчислювальні методології такого моделювання, а Wang et al. [35] розкрили можливості мультиплексних мереж для відображення міжсекторальних залежностей. Ці праці зміщують дослідницьку увагу з фізичного збереження окремого об'єкта на безперервність функцій і недопущення каскадної

кризи, проте недостатньо пов'язують відповідні показники з безпосереднім збереженням життя та здоров'я людини.

Людиноцентричний вимір досліджуваної проблеми набуває розвитку в межах концепції вітальної безпеки. У сучасних наукових працях переосмислено зміст безпеки людини в умовах гібридного миру та обґрунтовано вітальну безпеку як гнучку багатовимірну конструкцію, орієнтовану на збереження життя, здоров'я і життєвого потенціалу людини [26]. Подальший розвиток цієї концепції поглибив соціально-філософське розуміння взаємозв'язку вітальності, вітальної безпеки та життєстійкості людини в критичних життєвих ситуаціях [27]. Застосування зазначених положень у сфері боротьби з тероризмом розширює критерії оцінювання її результативності: поряд із кількістю виявлених загроз, припинених терористичних актів і проведених заходів мають визначатися здатність системи запобігати загибелі й травмуванню людей, зберігати їхнє здоров'я, гідність, життєвий потенціал і функціональну спроможність. Теоретичне осмислення вітальної безпеки ще не супроводжується комплексним розробленням поняття вітальної складової антитерористичної безпеки, визначенням її структури, вимірюваних показників та інституційних механізмів наукового забезпечення.

Інституційні джерела доповнюють наукову дискусію, визначаючи міжнародні орієнтири протидії тероризму. Глобальна контртерористична стратегія Організації Об'єднаних Націй поєднує запобігання тероризму, зміцнення державних спроможностей, забезпечення прав людини та усунення умов, сприятливих для поширення терористичних проявів [31; 32]. У дослідженні Міжрегіонального науково-дослідного інституту Організації Об'єднаних Націй із питань злочинності та правосуддя окреслено ризики злочинного використання алгоритмів поряд із потенціалом штучного інтелекту для аналізу загроз [33]. Документи Європейського Союзу розвивають правове регулювання протидії поширенню терористичного контенту та забезпечення стійкості критичних суб'єктів, а документи НАТО акцентують на технологічній адаптації, міжвідомчій і міжнародній взаємодії [11; 12; 22]. Функціональне призначення наведених міжнародних документів полягає передусім у встановленні політичних і правових орієнтирів протидії тероризму, тоді як визначення конкретної організаційної моделі наукового забезпечення та механізмів її функціонування залишається завданням кожної держави на національному рівні.

Проведений огляд показує, що сучасна наукова література містить вагомі результати щодо дослідження радикалізації, цифрового середовища, штучного інтелекту, кіберризиків, стійкості критичної інфраструктури та людиноцентричної безпеки. Наявність значних напрацювань в окремих тематичних сферах не супроводжується їх інтеграцією в цілісну систему наукового забезпечення боротьби з тероризмом, унаслідок чого відповідні напрями продовжують розвиватися переважно паралельно. Недостатньо дослідженим залишається механізм послідовного перетворення операційних даних суб'єктів боротьби з тероризмом на науково верифіковане знання, інноваційне рішення, практичне впровадження та вимірюваний результат. Не сформовано також цілісної моделі постійної взаємодії між координаційними органами, оперативними підрозділами, закладами освіти та науковими установами. Усунення виявленої теоретико-методологічної та інституційної невизначеності становить основне спрямування цього дослідження, у якому наука розглядається як системоутворювальна й випереджальна основа боротьби з тероризмом, а збереження людського життя — як визначальний критерій практичної ефективності антитерористичної діяльності.

Методологія дослідження

Дослідження виконано в межах концептуально-аналітичного огляду із цілеспрямованим відбором наукових джерел, застосуванням нормативно-правового аналізу, тематичного узагальнення та інституційного моделювання. Його спрямовано не на експериментальну

перевірку окремої контртерористичної технології, а на встановлення місця і функцій науки в загальнодержавній системі боротьби з тероризмом, визначення нормативних та організаційних прогалин і розроблення авторської моделі їх усунення. Емпіричний компонент у формі опитування, інтерв'ювання, спостереження або експерименту не застосовувався; експериментальну вибірку не формували. Джерельною основою стали відкриті наукові публікації, нормативно-правові акти й офіційні документи міжнародних організацій, доступні станом на 4 вересня 2026 року.

Методологічною основою дослідження є концептуально-аналітичний огляд із цілеспрямованим відбором джерел, орієнтований на зіставлення наукових положень, нормативних вимог та інституційних підходів для побудови авторської концепції наукового забезпечення боротьби з тероризмом. Логіка відбору визначається внеском джерела в розкриття дослідницької проблеми, обґрунтування функцій науки та пояснення зв'язків між даними, дослідженнями і практичними рішеннями. Наведені тематичні напрями, часові межі та критерії включення окреслюють межі аналітичного корпусу, проте не передбачають вичерпного охоплення всіх публікацій і не становлять протоколу систематичного огляду. Обґрунтованість концептуальних висновків оцінюється за простежуваністю їх зв'язку з використаними джерелами, послідовністю аргументації та відповідністю висновків можливостям застосованих методів. Описана процедура відбору й аналізу джерел забезпечує прозорість формування авторських положень, водночас залишаючи перевірку практичної результативності запропонованої моделі завданням подальших емпіричних досліджень.

До аналітичного корпусу включено 36 джерел: 22 рецензовані наукові публікації з DOI, шість нормативно-правових актів України та вісім документів або аналітичних матеріалів Європейського Союзу, ООН, UNICRI, НАТО й OECD. Основний часовий інтервал наукових публікацій охоплював 2021–2026 роки. Праці 2006 і 2020 років включено як методологічно значущі винятки, оскільки вони відображають фундаментальні проблеми доказовості й розвитку науки про тероризм [18; 29]. Для нормативних актів застосовано не часовий, а функціональний критерій: до корпусу включали чинні або концептуально важливі документи незалежно від року ухвалення.

Пошук і відбір матеріалів проводили за тематичними комбінаціями українських та англійських ключових слів: "наукове забезпечення боротьби з тероризмом", "антитерористична безпека", "тероризм і наука", "вітальна безпека", "людиноцентрична безпека", "counterterrorism science", "evidence-based counterterrorism", "terrorism research", "violent radicalization", "artificial intelligence and terrorism", "cyberterrorism", "critical infrastructure resilience" та "human security". Бібліографічні відомості й DOI звіряли за даними Crossref і сторінками видавців, а правові та інституційні документи — за офіційними ресурсами Верховної Ради України, Президента України, ЄС, ООН, НАТО та відповідних міжнародних установ.

Критеріями включення були: безпосередня відповідність меті дослідження; наявність повних і перевірюваних бібліографічних даних; рецензований характер наукової публікації або офіційний статус документа; висвітлення принаймні одного з визначених тематичних блоків; можливість установити зв'язок між досліджуваною проблемою та функціями наукового забезпечення. Перевагу надавали сучасним англомовним працям, систематичним оглядам і дослідженням із чітко описаною методологією. Виключали дублікати, неперевірені повідомлення, публіцистичні матеріали, джерела без установленого авторства або походження, а також праці, у яких тероризм згадувався лише побіжно. Матеріали з обмеженим доступом не використовували для формування перевірюваних висновків; безпеково чутливі питання аналізували виключно на концептуальному рівні.

Дослідження проведено у шість послідовних етапів. На першому етапі визначено предметні блоки аналізу: роль науки; прогнозування і радикалізація; цифрові та кібернетичні загрози; штучний інтелект; стійкість критичної інфраструктури; людиноцентрична й вітальна

безпека; інституційна організація наукового забезпечення. На другому етапі відібрано та класифіковано джерела відповідно до зазначених критеріїв. На третьому здійснено тематичне кодування їх змісту за категоріями “проблема”, “метод”, “науковий результат”, “практична функція”, “обмеження” та “можливість застосування в Україні”. На четвертому етапі проаналізовано законодавчо визначені функції і зв’язки суб’єктів боротьби з тероризмом. На п’ятому зіставлено наукові потреби з наявними нормативними та інституційними механізмами. На шостому сформовано концептуальні положення і трирівневу інституційну модель наукового забезпечення.

Для опрацювання матеріалів застосовано комплекс взаємопов’язаних методів. Контент-аналіз використано для виявлення основних напрямів, повторюваних положень і прогалин у наукових та інституційних джерелах. Порівняльний метод дав змогу зіставити підходи до радикалізації, використання ШІ, кіберризиків і стійкості інфраструктури, не ототожнюючи різні за природою загрози. Формально-юридичний метод застосовано для визначення нормативного змісту компетенцій, процедур і механізмів, закріплених у законодавстві України, зокрема в Положенні про єдину державну систему та Концепції боротьби з тероризмом в Україні [3; 6]. Інституційно-функціональний аналіз використано для встановлення відповідності між науковими функціями та суб’єктами, спроможними їх виконувати.

Системний підхід дозволив розглядати наукове забезпечення як безперервний цикл: отримання даних, їх наукове опрацювання, прогнозування, розроблення рішення, апробація, впровадження, оцінювання результату та коригування. Метод концептуалізації застосовано для уточнення змісту вітальної складової антитерористичної безпеки, а людиноцентричний підхід — для визначення життя, здоров’я, гідності й функціональної спроможності людини головними критеріями оцінювання антитерористичних рішень [26; 27]. Метод моделювання використано для побудови пропонованої трирівневої структури наукового забезпечення та розмежування її стратегічних, координаційно-виконавчих і освітньо-дослідних функцій.

Для систематизації матеріалу та забезпечення простежуваності аналітичних висновків результати кожного джерела узагальнювали в аналітичній матриці «норма або наукове положення — наукова функція — відповідальний суб’єкт — виявлена прогалина — авторська пропозиція — очікуваний вітальний ефект». Висновок про наявність прогалини формували за умови, що певна необхідна наукова функція була обґрунтована дослідженнями або міжнародними документами, але не мала чіткого постійного виконавця, процедури реалізації чи механізму оцінювання в українській системі. Авторські пропозиції перевіряли на внутрішню логічну узгодженість, недублювання чинних повноважень, функціональну необхідність і спрямованість на збереження життя людини.

Наведені пошукові терміни, часові межі, критерії відбору, тематичні категорії та структура аналітичної матриці дають змогу простежити логіку дослідження й повторно проаналізувати використаний корпус джерел, однак не гарантують отримання тотожного переліку матеріалів у разі нового пошуку. Оскільки дослідження ґрунтується виключно на відкритих документах і публікаціях та не передбачає залучення людей, оброблення персональних даних або проведення експериментів, отримання окремого схвалення комісії з етики не вимагалося.

Результати дослідження

1. Наука як системоутворювальна основа боротьби з тероризмом

Проведений аналіз дав змогу встановити, що наукове забезпечення боротьби з тероризмом не може розглядатися як сукупність епізодичних досліджень, експертних консультацій або навчально-методичних розробок. Системний характер наукового забезпечення виявляється в безперервному здобутті, перевірці, систематизації та практичному застосуванні знань про терористичні загрози, уразливості об’єктів, поведінку суб’єктів терористичної діяльності,

наслідки терористичних актів і результативність заходів реагування. Зазначений процес охоплює фундаментальні, прикладні, пошукові, прогностичні, експертні, дослідно-конструкторські й освітні компоненти, об'єднані спільною метою — випередженням терористичних загроз і збереженням людського життя.

Визначення предметних меж наукового забезпечення потребує попереднього уточнення місця антитерористичної безпеки в системі державної безпеки. Антитерористичну безпеку запропоновано розглядати як функціональну складову державної безпеки, спрямовану на захист держави, суспільства та людини шляхом науково обґрунтованого прогнозування, запобігання, своєчасного виявлення і припинення реальних та потенційних терористичних загроз, а також мінімізації спричинених ними наслідків. Уточнення змісту цієї категорії дає змогу сформулювати поняття її наукового забезпечення.

Наукове забезпечення боротьби з тероризмом — це організована, безперервна та захищена система вироблення, перевірки, систематизації, впровадження й оцінювання наукових знань, методів і технологій, спрямована на прогнозування терористичних загроз, запобігання їм, захист людини та об'єктів можливих терористичних посягань, підвищення ефективності стратегій реагування і мінімізації наслідків терористичної діяльності з неухильним дотриманням прав і свобод людини.

Запропоноване визначення потребує розмежування взаємопов'язаних, але не тотожних категорій. **Наукове забезпечення** охоплює цілісну систему вироблення, перевірки, застосування та оцінювання доказово обґрунтованих знань. **Науковий супровід** є складовою наукового забезпечення і полягає в дослідницькій, методичній та експертній підтримці конкретного процесу, заходу, технології або управлінського рішення. **Інноваційна діяльність** забезпечує перетворення наукового знання на новий або істотно вдосконалений метод, продукт, технологію чи організаційне рішення. **Трансфер наукових результатів** означає їх передання, адаптацію та практичне впровадження в діяльність суб'єктів боротьби з тероризмом. **Оцінювання ефективності** передбачає перевірку фактичного впливу впровадженого рішення на рівень ризику, своєчасність реагування, стійкість захищуваних функцій, а також збереження життя і здоров'я людини. Визначення функціонального призначення та послідовності реалізації кожної із зазначених категорій унеможливлює ототожнення створення наукової розробки з її практичним упровадженням, а факту впровадження — з наявністю доведеної ефективності.

Системоутворювальна роль науки проявляється в тому, що вона формує спільну доказову основу для різних суб'єктів боротьби з тероризмом. Оперативна, розвідувальна, контррозвідувальна, правоохоронна, військова, рятувальна, інформаційна й освітня діяльність мають різні завдання, процедури та джерела даних. Без наукового узагальнення результати цієї діяльності залишаються відомчо роз'єднаними, а накопичений досвід не завжди перетворюється на відтворюване знання. Наука забезпечує понятійну узгодженість, порівнянність оцінок, перевірку гіпотез, побудову сценаріїв та обґрунтування критеріїв, за якими можна визначити, чи зменшило конкретне рішення ймовірність терористичного акту або тяжкість його наслідків.

Механізм системоутворювального впливу науки полягає у формуванні зв'язків, через які практичні потреби визначають дослідницькі завдання, результати досліджень обґрунтовують управлінські й технологічні рішення, а оцінені наслідки їх застосування стають підставою для коригування підходів до прогнозування, підготовки та реагування. Завдяки цим зв'язкам досвід одного суб'єкта після наукової перевірки може ставати підставою для вдосконалення діяльності інших, забезпечуючи накопичення знань і адаптацію системи загалом. За відсутності такого механізму адміністративна координація може зберігатися, однак розривається послідовність між виявленням проблеми, обґрунтуванням рішення та перевіркою його наслідків, унаслідок чого послаблюється здатність системи до доказово

обґрунтованого самокоригування. З огляду на зазначені взаємозв'язки системоутворювальний статус науки визначається її функцією забезпечення міжвідомчого поширення та застосування перевіреного досвіду, а також зворотного впливу результатів практики на спільні правила діяльності. У межах запропонованої концепції цей механізм дає підстави розглядати наукове забезпечення як основу цілісності й адаптивності антитерористичної системи.

Первинність науки має функціональний, а не адміністративний зміст. Функціональна пріоритетність наукового забезпечення не підміняє компетенції уповноважених органів і не передбачає втручання в безпосереднє оперативне управління. Зміст зазначеного принципу полягає в тому, що до нормативного закріплення, фінансування чи масштабування антитерористичного рішення повинні бути науково визначені проблема, мета, допустимий ризик, можливі альтернативи, очікуваний ефект і ймовірні негативні наслідки. Після впровадження відповідного рішення наука має забезпечувати оцінювання одержаного результату та перевірку вихідних припущень. Поєднання попереднього наукового обґрунтування антитерористичного рішення з подальшим оцінюванням результатів його практичного впровадження відповідає визначеній у міжнародних дослідженнях потребі посилення доказовості контртерористичних програм, значна частина яких досі не має належного методологічного оцінювання ефективності [20; 19].

На цій основі сформовано функціональну модель науки в боротьбі з тероризмом, яка охоплює сім взаємопов'язаних функцій: пізнавальну — встановлення природи, причин і механізмів загрози; прогностичну — передбачення її трансформацій; аналітичну — опрацювання даних і виявлення закономірностей; технологічну — розроблення засобів та алгоритмів; експертно-оцінювальну — перевірку обґрунтованості й результативності рішень; освітню — формування професійних і суспільних компетентностей; людиноцентричну — співвіднесення кожного рішення з його впливом на життя, здоров'я, гідність і права людини. Неповна реалізація зазначених функцій створює ризик порушення повноти дослідницького циклу: недостатність даних послаблює обґрунтованість прогнозу, відсутність валідації технології залишає невизначеними ризики її застосування, а брак оцінювання практичних результатів обмежує можливості перевірки та коригування рішень.

Освітня та пізнавальна функції наукового забезпечення охоплюють також професіологічний та акмеологічний виміри антитерористичної діяльності. Технологічний розвиток не забезпечує належної ефективності без відповідного професійного розвитку фахівця, його психологічної готовності, здатності критично оцінювати інформацію, працювати в команді та ухвалювати правомірні рішення в умовах дефіциту часу, невизначеності й високого ризику. Професійність у цій сфері слід розглядати не як одноразово підтверджену кваліфікацію, а як безперервний процес формування і вдосконалення компетентностей, стресостійкості, ситуаційної обізнаності та спроможності до міжвідомчої взаємодії. Визнання професійності безперервним процесом розвитку зумовлює необхідність включення до наукового забезпечення досліджень людського чинника й організаційної надійності, моделювання екстремальних ситуацій, психологічної підготовки, командних навчань та аналізу рішень, ухвалених у реальних і навчальних умовах. Людиноцентричний зміст освітньої функції наукового забезпечення не обмежується підготовкою фахівців, а поширюється також на формування спеціальних знань і практичних навичок населення. Здатність людини своєчасно розпізнати загрозу, виконати алгоритм безпечної поведінки, уникнути панічних дій і не поширювати дезінформацію безпосередньо впливає на вітальний результат антитерористичних заходів.

2. Цикл перетворення даних на антитерористичне рішення

Наукове забезпечення запропоновано організувати як безперервний цикл: "операційні дані — науковий аналіз — прогноз — розроблення рішення — апробація — впровадження —

оцінювання — коригування". Початковим ресурсом цього циклу є не лише інформація про вчинені терористичні акти, а й відомості про підготовчі дії, зміни способів радикалізації, джерела фінансування, цифрові комунікації, уразливості критичної інфраструктури, результати навчань, помилкові сигнали та відвернені загрози. До дослідницького масиву необхідно також включати негативні результати й випадки, у яких прогноз не підтвердився або застосований захід не забезпечив очікуваного ефекту. Опрацювання таких відомостей дає змогу виявляти систематичні помилки, уточнювати дослідницькі припущення та запобігати завищенню результативності застосовуваних інструментів.

На етапі наукового аналізу дані повинні очищуватися від дублікатів, класифікуватися за уніфікованими ознаками та перевірятися на повноту, достовірність, актуальність і репрезентативність. Прогностичний етап передбачає не встановлення неминучої поведінки конкретної особи, а формування ймовірнісних сценаріїв із визначенням відповідних умов, індикаторів і меж невизначеності. Багатофакторна природа радикалізації та залежність ризикових профілів від соціального й поведінкового контексту виключають використання окремої ознаки як достатньої підстави для висновку про наявність терористичної загрози [38; 8]. Імовірнісний і контекстуально залежний характер прогнозування визначає допоміжне призначення наукового прогнозу: він має забезпечувати аналітичну підтримку професійного рішення, а не автоматично підмінювати його.

Розроблене рішення потребує попередньої апробації за допомогою модельних сценаріїв, під час навчань, на контрольованих вибірках або в межах пілотних проєктів. Перехід від експериментальної апробації рішення до його масштабного впровадження може здійснюватися лише після перевірки функціональної придатності, правомірності й ресурсної обґрунтованості, а також оцінювання можливого впливу на права людини. Завершальне оцінювання повинно встановлювати не тільки факт виконання запланованого заходу, а й фактичну зміну рівня ризику, своєчасність реагування, стійкість захищуваної функції та досягнутий вітальний ефект. Одержані результати повертаються до початкового етапу у формі уточнених даних і стають підставою для коригування прогнозів, методик, технологій та організаційних процедур.

Функціонування зазначеного циклу потребує належно **організованої інформаційної логістики**, під якою в межах цього дослідження запропоновано розуміти керований процес збирання, перевірки, структурування, захищеного зберігання, передавання й аналітичного опрацювання даних для своєчасного забезпечення суб'єктів боротьби з тероризмом інформацією, необхідною для ухвалення рішень. Її призначення полягає не в механічному накопиченні відомостей, а в перетворенні різнорідних даних на достовірне, контекстуалізоване та придатне до практичного використання знання. Залежно від характеру загрози й поставленого завдання відповідна інформація має надходити в реальному або максимально наближеному до реального часі з дотриманням установлених режимів доступу та вимог щодо захисту персональних даних.

Ключовою умовою дієвості інформаційної логістики є міжсистемна сумісність її технологічних, організаційних і семантичних складових. Міжсистемна сумісність передбачає узгодженість форматів даних, класифікаторів, критеріїв оцінювання, каналів захищеного обміну, повноважень учасників і процедур перевірки інформації. Наукові дослідження кіберризиків засвідчують, що неоднорідність, неповнота й обмежена доступність даних ускладнюють побудову надійних моделей, тоді як ефективність методів оцінювання залежить від їх призначення, ресурсомісткості та практичної застосовності [9; 17]. Урахування зазначених обмежень зумовлює необхідність оцінювати сумісність не лише за технічною здатністю систем обмінюватися відомостями, а й за узгодженістю розуміння змісту даних, можливістю перевірки їх походження та належністю використання в межах визначених управлінських процедур.

Проведений нормативно-функціональний аналіз дає підстави констатувати наявність ризику фрагментарності інформаційного обміну між суб'єктами боротьби з тероризмом, проте фактичний масштаб відповідної проблеми потребує окремого емпіричного оцінювання. Виявлений ризик визначає формування захищеного міжвідомчого інформаційного середовища як один із пріоритетних напрямів розвитку наукового забезпечення. Відповідне середовище має забезпечувати сумісність даних, їх контрольоване використання та простежуваність процесу перетворення первинного повідомлення на науково обґрунтоване рішення. Створення та функціонування захищеного міжвідомчого інформаційного середовища не передбачає необмеженого об'єднання всіх інформаційних ресурсів або встановлення однакового доступу для всіх учасників. Обсяг доступних відомостей має визначатися компетенцією відповідного суб'єкта, метою їх використання, рівнем чутливості інформації та встановленим режимом секретності.

Встановлений взаємозв'язок між збиранням, опрацюванням і практичним використанням даних дає підстави розглядати інформаційну логістику як інфраструктурну основу функціонування сформованого наукового циклу, що забезпечує послідовне перетворення даних на інформацію, інформації — на перевірене знання, а знання — на практичне антитерористичне рішення. Якість, своєчасність, достовірність і міжсистемна сумісність даних безпосередньо визначають здатність науки не лише пояснювати вже реалізовані загрози, а й завчасно розробляти обґрунтовані засоби їх прогнозування, запобігання та нейтралізації.

3. Вітальна складова антитерористичної безпеки

Вітальна складова антитерористичної безпеки — це людиноцентричний компонент системи запобігання, виявлення і припинення терористичної діяльності та мінімізації її наслідків, спрямований на пріоритетне збереження життя, здоров'я, гідності, життєвого потенціалу та функціональної спроможності людини. Її зміст не обмежується фізичним виживанням під час терористичного акту. Він охоплює зменшення ймовірності потрапляння людини в зону ураження, своєчасне попередження й евакуацію, доступність допомоги, захист життєво важливих послуг, недопущення вторинних втрат, психологічне відновлення та збереження правових гарантій.

Наукове забезпечення вітальної складової антитерористичної безпеки становить організовану діяльність із розроблення, перевірки та впровадження знань, критеріїв, методик і технологій, за допомогою яких вплив антитерористичних рішень оцінюється за їхньою здатністю зберігати життя, здоров'я, гідність, життєвий потенціал і функціональну спроможність людини.

Запропоноване розуміння розвиває концепцію вітальної безпеки, у якій безпека людини пов'язується зі збереженням її життєвого потенціалу й здатністю підтримувати основні функції в умовах гібридних і критичних загроз [26; 27]. Стосовно боротьби з тероризмом це означає зміну критерію результативності. Кількість проведених перевірок, навчань, заблокованих повідомлень або встановлених технічних засобів характеризує обсяг діяльності, але не доводить досягнення безпекового результату. Необхідно встановлювати, яким чином ці дії зменшили ризик загибелі, травмування, паніки, тривалого припинення медичної допомоги, водопостачання, енергозабезпечення або зв'язку.

Вітальний ефект запропоновано розглядати через чотири взаємопов'язані групи критеріїв. Перша охоплює превентивний ефект — зменшення ймовірності реалізації загрози та скорочення кількості осіб, які можуть зазнати ураження. Друга відображає захисний ефект — спроможність об'єкта, персоналу й населення діяти під час загрози. Третя характеризує рятувально-відновний ефект — своєчасність допомоги, збереження критичних функцій і недопущення каскадних наслідків. Четверта визначає правозахисний ефект — пропорційність обмежень, недискримінацію, захист даних і можливість перевірки рішень. Відтак людиноцентричність не

протиставляється державній безпеці, а конкретизує її кінцеве призначення: безпека держави набуває практичного змісту через здатність захищати життя людини.

Для переходу від концептуального визначення вітального критерію до його практичного застосування запропоновано початкову систему показників, яка конкретизує превентивний, захисний, рятувально-відновний і правозахисний ефекти антитерористичних рішень. Вітальний критерій визначає спрямованість оцінювання на збереження життя, здоров'я, гідності та функціональної спроможності людини, тоді як показники відображають окремі вимірювані прояви цього результату. Операціоналізація передбачає встановлення змісту кожного показника, одиниці вимірювання, джерела даних, бажаного напряму зміни та правила оцінювання. Запропонована система має концептуальний характер і становить основу для розроблення та пілотної перевірки відповідної методики.

Одиницею оцінювання доцільно визначати конкретне антитерористичне рішення, програму або комплекс заходів щодо певного об'єкта, території чи групи населення. До початку оцінювання необхідно зафіксувати сценарій загрози, період спостереження, чисельність і склад населення, умови функціонування об'єкта та вихідні значення показників. Порівняння має здійснюватися за зіставних умов, оскільки зміна інтенсивності загрози, кількості людей або доступності ресурсів може впливати на результат незалежно від застосованого рішення. Оцінюванню підлягають наслідки як самої терористичної загрози, так і заходів протидії їй, включно з можливими вторинними втратами та несприятливим впливом на залучених фахівців. Запропоновані показники вітального ефекту, одиниці їх вимірювання, джерела даних, бажані напрями зміни та правила оцінювання систематизовано в таблиці.

Таблиця. Операціоналізація вітального критерію антитерористичної безпеки

Вимір вітального ефекту	Показник та його зміст	Одиниця вимірювання	Джерело даних	Бажаний напрям зміни	Правило оцінювання
Превентивний і захисний	**Ризик загибелі:** оцінена ймовірність загибелі особи за визначений період з урахуванням сценарію загрози та заходів захисту	Імовірність від 0 до 1 або %	Сценарні моделі; знеособлені дані про інциденти; характеристики об'єкта та захисних заходів	Зменшення	Порівняння вихідного й залишкового ризику за однакових сценарних припущень; зазначення невизначеності оцінки
Превентивний і захисний	**Ризик травмування:** оцінена ймовірність отримання травми визначеної тяжкості за встановлений період	Імовірність від 0 до 1 або %, окремо за тяжкістю травм	Сценарні моделі; знеособлені медичні дані та матеріали аналізу інцидентів	Зменшення	Зіставлення ризику до і після застосування рішення; окреме оцінювання тяжких наслідків
Превентивний	**Чисельність населення під ризиком:** кількість людей у визначеній зоні можливого ураження або небезпечного порушення життєво важливої послуги	Особи; % від визначеної групи населення	Просторові моделі; дані про перебування людей; відомості операторів послуг	Зменшення	Визначення кількості та частки осіб під ризиком без повторного обліку; окреме врахування груп із підвищеною вразливістю

Вимір вітального ефекту	Показник та його зміст	Одиниця вимірювання	Джерело даних	Бажаний напрям зміни	Правило оцінювання
Захисний	**Готовність до безпечних дій:** частка осіб, які під час практичної перевірки правильно виконали визначений алгоритм оповіщення, укриття або евакуації	% перевірених осіб	Протоколи навчань; спостереження за практичними вправами	Збільшення	Порівняння з попередньо визначеним еталоном виконання; критичні помилки фіксуються окремо
Рятувально-відновний	**Своєчасність допомоги:** частка постраждалих, які отримали необхідну допомогу в межах визначеного для відповідного стану часу	% постраждалих; хвилини очікування	Знеособлені записи екстрених служб; журнали реагування; матеріали навчань	Збільшення частки своєчасної допомоги; скорочення затримок	Оцінювання за категоріями потреби в допомозі; окремий облік випадків ненадання або критичного запізнення
Рятувально-відновний	**Недоступність життєво важливої послуги:** сумарна тривалість її відсутності або надання нижче мінімально безпечного рівня протягом періоду спостереження	Хвилини або години; додатково — людино-години недоступності	Журнали операторів; системи моніторингу; дані про населення, залежне від послуги	Зменшення	Зіставлення з допустимою тривалістю переривання; урахування кількості людей, для яких послуга була недоступною
Захисний і рятувально-відновний	**Доступність резервної послуги:** частка населення, забезпечена альтернативним джерелом життєво важливої послуги на мінімально безпечному рівні	% населення, яке потребує послуги	Дані операторів; перевірки резервних систем; результати навчань	Збільшення	Перевірка фактичної доступності та достатності резерву для визначеної потреби
Рятувально-відновний	**Час відновлення мінімально безпечного функціонування:** період від порушення функції до стійкого досягнення визначеного мінімального рівня	Хвилини або години	Журнали інцидентів і відновлення; технічний моніторинг; матеріали навчань	Зменшення	Порівняння з попередньо встановленим граничним часом; фіксація моментів порушення та підтвердженого відновлення

Вимір вітального ефекту	Показник та його зміст	Одиниця вимірювання	Джерело даних	Бажаний напрям зміни	Правило оцінювання
Рятувально-відновний	**Збереження функціональної спроможності:** частка постраждалих, які у визначений строк зберегли або відновили здатність до повсякденної діяльності за обраним стандартизованим інструментом	% обстежених постраждалих	Знеособлені результати медичного, психологічного та реабілітаційного оцінювання	Збільшення	Зіставлення результатів за однаковим інструментом і строком спостереження; зазначення повноти охоплення постраждалих
Правозахисний	**Частота підтверджених порушень правових гарантій:** частка перевірених рішень із підтвердженими порушеннями вимог законності, пропорційності, недискримінації або захисту даних	% перевірених рішень; кількість і тяжкість порушень	Результати незалежної перевірки; остаточні рішення уповноважених органів	Зменшення до відсутності підтверджених порушень	Оцінювання за визначеними вимогами та зіставного охоплення перевіркою; тяжкі порушення розглядаються окремо

Джерело: авторська концептуальна розробка. Наведені джерела даних визначають можливу інформаційну основу майбутнього оцінювання і не означають, що відповідні дані були зібрані в цьому дослідженні.

Застосування таблиці передбачає розмежування прогнозних оцінок і фактично зафіксованих наслідків. Ризик загибелі та травмування є модельними показниками, достовірність яких залежить від якості даних, обґрунтованості сценарію та перевірки застосованої моделі. Фактичні випадки загибелі й травмування необхідно обліковувати окремо із зазначенням тяжкості наслідків, чисельності населення під впливом загрози та періоду спостереження. Відсутність людських втрат сама по собі не підтверджує ефективності рішення, так само як їх наявність без урахування інтенсивності загрози не доводить його неефективності. Результати навчань характеризують готовність до дій, але не можуть без додаткової перевірки ототожнюватися з ефектом у реальних умовах.

Для кожного показника доцільно визначати вихідне значення, цільовий орієнтир і, за можливості, гранично неприйнятне значення. Їх обґрунтування має враховувати характер загрози, сектор діяльності, потреби залежного від послуги населення та наявні правові й технічні вимоги. На початковому етапі оцінювання пропонується подавати фактичне або модельне значення показника, його абсолютну зміну щодо вихідного рівня та відповідність установленому орієнтиру. Відносну зміну можна визначати лише за ненульового вихідного значення.

Якщо для порівняння потрібне приведення кількісних показників до спільної шкали, пропонується нормування в інтервалі від 0 до 1: значення 0 відповідає попередньо визначеній неприйнятній межі, а 1 — досягненню цільового орієнтира. Проміжне значення визначається за положенням показника між цими межами з урахуванням того, чи є бажаним його

зменшення або збільшення. Межі нормування мають залишатися однаковими для зіставлюваних варіантів і періодів; вихідні значення та випадки виходу за встановлені межі зберігаються у звіті. Таке нормування є способом упорядкування оцінок і потребує перевірки чутливості результатів до обраних орієнтирів.

Показники доцільно подавати як профіль результатів за окремими вимірами, без їх автоматичного зведення до єдиного інтегрального бала. Скорочення часу відновлення послуги не може компенсувати порушення прав людини або зростання ризику тяжких людських втрат. За відсутності достатніх даних показник позначається як такий, що не підлягає надійному оцінюванню, із зазначенням причини; відсутні відомості не прирівнюються до нульового ризику чи відсутності порушень. Поряд із загальними значеннями необхідно аналізувати результати для груп із підвищеною вразливістю, щоб середня оцінка не приховувала нерівномірності захисту.

Висновок про вітальну ефективність рішення має ґрунтуватися на сукупності показників, якості доказів та врахуванні альтернативних пояснень одержаного результату. Порівняння стану до і після впровадження відображає динаміку, але саме по собі не встановлює причинного впливу рішення; для цього, за можливості, необхідні зіставна група, контрольний сценарій або інший обґрунтований дизайн оцінювання. Науковий внесок запропонованої операціоналізації полягає у встановленні зв’язку між людиноцентричною метою антитерористичної діяльності, вимірюваними проявами її результату та правилами інтерпретації доказів. Експертна перевірка, уточнення показників і порогових значень, оцінювання доступності даних та пілотна апробація становлять наступний етап розроблення методики.

4. Технологічна трансформація терористичних загроз і роль ШІ

Аналіз сучасних досліджень засвідчив, що технологічна перевага у сфері боротьби з тероризмом не є сталою або винятково державною. Цифрові інструменти, системи штучного інтелекту та технології подвійного призначення можуть використовуватися державними органами, науковими установами, приватними компаніями й одночасно суб’єктами терористичної діяльності. Поширення однакових технологічних можливостей серед суб’єктів із принципово протилежними цілями породжує асиметричні безпекові наслідки: суб’єктові терористичної діяльності достатньо виявити й використати окрему вразливість, тоді як держава повинна забезпечувати стійкість усієї системи, законність застосовуваних засобів і належний захист прав людини.

Генеративний штучний інтелект знижує ресурсні, мовні та технічні бар’єри для створення багатомовного контенту, персоналізації повідомлень, виготовлення синтетичних аудіовізуальних матеріалів і автоматизації комунікацій. Небезпека використання генеративних моделей суб’єктами терористичної діяльності полягає не лише в можливості виникнення принципово нових форм протиправної активності, а й у прискоренні, масштабуванні та ситуативній адаптації вже відомих способів пропаганди, дезінформації, вербування і психологічного впливу [16; 14].

Weimann et al. [36] експериментально дослідили можливості зловмисного використання п’яти платформ на основі великих мовних моделей. Перевірка охоплювала запити, пов’язані з поляризаційним та емоційним контентом, дезінформацією, вербуванням, набуттям тактичних знань і плануванням нападів. Отримані результати виявили неоднакову стійкість платформ до прямих, непрямих і маніпулятивно сформульованих запитів, а також показали, що наявність формальних обмежень не гарантує неможливості генерування небезпечного змісту. Це підтверджує необхідність постійного наукового тестування захисних механізмів генеративних моделей, обміну інформацією про виявлені вразливості та співпраці державних органів, розробників технологій і дослідницьких установ.

Поряд із ризиками штучний інтелект розширює спроможності суб’єктів боротьби з тероризмом щодо опрацювання великих масивів різнорідних даних, виявлення аномалій,

аналізу мережевих зв'язків, розпізнавання синтетичного контенту та моделювання сценаріїв. Одним із перспективних напрямів є науковий моніторинг теророгенного потенціалу соціальних систем, під яким доцільно розуміти систематичне спостереження за сукупністю просторових, часових, соціальних, демографічних, економічних, інформаційних і безпекових індикаторів, зміни яких можуть свідчити про підвищення ймовірності проявів терористичної активності. Функціональне призначення наукового моніторингу теророгенного потенціалу полягає у своєчасному виявленні небезпечних тенденцій, формуванні обґрунтованих прогнозів і забезпеченні інформаційної підтримки превентивних рішень, а не в автоматичному визначенні конкретної особи як потенційного правопорушника.

Можливість практичного застосування відповідного підходу продемонстровано в дослідженні Python et al. [25], автори якого порівняли теоретично обґрунтовані статистичні моделі та алгоритми машинного навчання для прогнозування недержавного тероризму. На основі загальнодоступних даних моделі враховували не лише відомості про попередні терористичні події, а й структурні та динамічні характеристики досліджуваного середовища, зокрема просторове розташування, щільність населення, демографічні, соціально-економічні та безпекові показники. Результати засвідчили можливість формування інтерпретованих локальних прогнозів імовірності терористичної активності на один тиждень уперед, передусім у регіонах із відносно високою поширеністю відповідних проявів. У цих регіонах теоретично обґрунтовані моделі виявилися результативнішими за підходи, побудовані виключно на даних про попередні напади. Використання інтерпретованих просторово-часових прогностичних моделей може сприяти визначенню територій підвищеного ризику, обґрунтуванню превентивних заходів і раціональному розподілу ресурсів суб'єктів боротьби з тероризмом. Одержані за їх допомогою прогнози повинні використовуватися як інструмент підтримки професійного рішення, а не як безумовне передбачення конкретного терористичного акту [25].

Науково коректна інтерпретація одержаних результатів потребує врахування меж їх прогностичної достовірності, оскільки відповідне дослідження не доводить універсальної здатності штучного інтелекту точно передбачати конкретний терористичний акт. Прогностична придатність моделі залежить від повноти й достовірності вихідних даних, обраного просторового та часового масштабу, стабільності встановлених закономірностей і відповідності алгоритму новому середовищу використання. Недостатня представленість окремих регіонів у вихідних даних, зміна тактики суб'єктів терористичної діяльності або поява нових чинників можуть істотно знижувати точність прогнозування. Залежність прогностичної точності від зазначених умов означає, що алгоритмічний результат має відображати оцінену ймовірність і сценарні межі загрози, але не може розглядатися як безумовний доказ або самостійна правова підстава для обмеження прав конкретної особи.

Для суб'єктів боротьби з тероризмом алгоритмічний висновок повинен залишатися одним з елементів комплексної оцінки, оскільки він є похідним від якості навчальних даних, коректності обраних ознак і контексту застосування. Помилка у цій сфері може спричинити як невиявлення реальної загрози, так і необґрунтоване втручання у права людини. Через це технологічна новизна рішення не може бути самостійною підставою для його практичного впровадження. Обов'язковими умовами мають бути попередня валідація, тестування на алгоритмічне зміщення, пояснюваність результатів, документування версій моделі, захищеність від маніпулятивного впливу, реальний людський контроль і періодичне оцінювання результативності [30; 34].

У вітальному вимірі оцінюванню підлягає не тільки точність алгоритму, а й можливий вплив прийнятого на його основі рішення на життя, здоров'я, гідність і функціональну спроможність людини. Наукова перевірка має охоплювати два взаємопов'язані типи помилок: хибнонегативний результат, через який реальна загроза залишається невиявленою, та хибнопозитивний результат, здатний спричинити безпідставне втручання, стигматизацію або

нераціональне використання сил і засобів. Співвідношення цих ризиків необхідно визначати з урахуванням характеру загрози, тяжкості можливих наслідків і принципу пропорційності.

Отримані результати підтверджують потребу в постійній науковій структурі, спроможній поєднувати технологічну розробку з оперативною потребою, правовою та етичною оцінкою, вимогами інформаційної безпеки й вітальним критерієм. Без такого поєднання інформаційні системи можуть створюватися відокремлено, використовувати несумісні набори даних або оцінюватися лише за показниками технічної точності без урахування наслідків практичного рішення. Наукове забезпечення інформаційної безпеки має охоплювати дослідження цифрової радикалізації, виявлення координованої інформаційної активності, протидію синтетичному контенту, захист інформаційних систем та оцінювання впливу контрзаходів на законну комунікацію. Участь приватних платформ потребує спеціальних процедур прозорості та підзвітності, оскільки застосовувані ними алгоритми модерації фактично впливають на реалізацію антитерористичної політики [7].

5. Науково-інноваційний контур боротьби з тероризмом

Проведений аналіз засвідчив, що інноваційне забезпечення боротьби з тероризмом не може зводитися до придбання новітнього обладнання, програмного забезпечення або механічного запозичення іноземних технологій. Технологічна новизна не є самостійним доказом безпечності та практичної результативності рішення. Інновація набуває антитерористичної цінності лише тоді, коли вона відповідає встановленій загрозі, пройшла наукову, правову, етичну й безпекову перевірку, підтвердила ефективність у контрольованих умовах та може бути інтегрована в діяльність відповідних суб’єктів без створення неприйнятних ризиків для людини.

На цій підставі запропоновано розглядати науково-інноваційний контур як послідовність взаємопов’язаних етапів: виявлення практичної або технологічної потреби; формування наукового й технічного завдання; пошук наявних рішень; розроблення концепції або прототипу; лабораторне чи модельне випробування; правова, етична та безпекова експертиза; пілотна апробація; оцінювання фактичного ефекту; прийняття рішення про масштабування, доопрацювання або припинення використання. Після впровадження технологія повинна підлягати періодичній повторній перевірці, оскільки зміна характеру загроз, структури даних або середовища застосування може знизити її точність і надійність.

До перспективних напрямів інноваційної діяльності належать системи прогнозного аналізу, автоматизованого виявлення аномалій, моніторингу цифрового середовища, аналізу мережевих зв’язків і фінансових операцій, розпізнавання синтетичного контенту, захисту інформаційно-комунікаційних систем, моделювання поведінки взаємозалежної критичної інфраструктури, роботизованого обстеження небезпечних об’єктів, дистанційного виявлення вибухових, хімічних і біологічних загроз, підтримки кризових комунікацій та мінімізації наслідків терористичних актів. Безпечна реалізація перелічених інноваційних напрямів потребує визначення конкретних характеристик відповідних засобів із дотриманням установлених режимних обмежень, вимог щодо захисту інформації та недопущення розкриття відомостей про вразливості, методи виявлення загроз і можливі способи обходу захисних механізмів.

Результативність інноваційного рішення запропоновано оцінювати за сукупністю взаємопов’язаних критеріїв: точністю і стійкістю одержаних результатів; скороченням часу виявлення загрози та реагування на неї; сумісністю з наявними інформаційними й управлінськими системами; ресурсною обґрунтованістю; можливістю проведення аудиту; дотриманням законності та прав людини; зменшенням ризику загибелі, травмування або втрати функціональної спроможності людини. Оцінювання за наведеною системою критеріїв дає підстави стверджувати, що факт придбання технології, завершення дослідно-конструкторської роботи або видання акта про впровадження не може автоматично визнаватися підтвердженням її ефективності. Обов’язковою умовою такого підтвердження є

встановлення вимірюваного безпекового й вітального ефектів у реальних або максимально наближених до них умовах практичної діяльності.

Послідовне проходження всіх етапів науково-інноваційного контуру створює об'єктивні підстави для розмежування експериментальної розробки, апробованого рішення та підтвердженої інновації. Експериментальна розробка характеризується науково обґрунтованим потенціалом, але ще не проходила необхідних випробувань; апробоване рішення підтвердило свою працездатність у контрольованих або пілотних умовах; підтверджена інновація продемонструвала вимірюваний безпековий і вітальний ефекти під час практичного застосування. Установлення об'єктивних критеріїв відповідності кожній із зазначених стадій запобігає підміні реального технологічного розвитку формальними показниками та забезпечує спрямування ресурсів на рішення, спроможні відповідати динаміці трансформації терористичних загроз і зміцнювати вітальну складову антитерористичної безпеки.

6. Наукове забезпечення стійкості критичної інфраструктури у вітальному вимірі антитерористичної безпеки

Науковий результат у сфері захисту критичної інфраструктури полягає в переході від об'єктового до функціонального підходу. Фізична неушкодженість об'єкта не гарантує збереження відповідної послуги, якщо порушено зовнішнє енергопостачання, зв'язок, логістику або доступ персоналу. Збереження життєво важливої функції можливе навіть за часткового пошкодження об'єкта завдяки резервуванню, розосередженню ресурсів чи використанню альтернативних маршрутів. Виявлена невідповідність між фізичним станом об'єкта та його функціональною спроможністю зумовлює необхідність визначати критичність не лише за характеристиками споруди, а й за суспільним значенням виконуваної функції, міжсекторальними залежностями, допустимим часом її переривання та масштабом можливих людських втрат.

Моделювання взаємозалежностей дозволяє виявляти точки, відмова яких породжує каскадні наслідки, та обґрунтовувати пріоритетність захисту і відновлення [37; 35]. Розроблені в науковій літературі індикатори стійкості охоплюють готовність, здатність поглинати вплив, відновлюватися та адаптуватися, але потребують секторальної й національної конкретизації [28; 24]. Для антитерористичної безпеки таку конкретизацію запропоновано здійснювати через вітальні наслідки: кількість людей, залежних від функції; швидкість переходу технічного порушення у загрозу життю; доступність резервної послуги; час, необхідний для відновлення мінімально безпечного рівня функціонування.

Нормативне підґрунтя для застосування такого підходу закладено у Правилах антитерористичної безпеки, затверджених постановою Кабінету Міністрів України від 15 жовтня 2024 року № 1172. Правила передбачають формування прогнозованої загрози як моделі можливих максимально негативних наслідків терористичних посягань відповідно до наявних загроз щодо конкретного об'єкта. Під час її формування аналізуються характеристики об'єкта, проєктна документація, технологічні регламенти та інші матеріали, пов'язані з його експлуатацією, виявляються найбільш уразливі місця, визначаються ймовірні способи посягання та прогнозуються людські, економічні, екологічні й суспільно-політичні втрати [4]. Виконання цих завдань не повинно зводитися до формального заповнення передбачених документів, оскільки вибір сценарію, встановлення взаємозалежностей, оцінювання можливих наслідків і перевірка вихідних припущень потребують міждисциплінарного наукового забезпечення. У вітальному вимірі пріоритетного значення набуває обґрунтоване прогнозування людських втрат, визначення часу переходу порушення роботи об'єкта у безпосередню загрозу життю та розроблення заходів, здатних запобігти таким наслідкам.

Установлено, що науковий супровід повинен охоплювати повний цикл захисту критичної інфраструктури: сценарне моделювання, оцінювання уразливостей, проєктування резервування, підготовку персоналу, проведення міжсекторальних навчань, аналіз фактичних

інцидентів і коригування паспортів безпеки. Вітальна складова такого супроводу має охоплювати не лише безперервність життєво важливих послуг для населення, а й безпосередній захист працівників, відвідувачів та інших осіб, які перебувають на відповідному об’єкті або в зоні можливого ураження. Науково обґрунтованими мають бути порядок своєчасного оповіщення, маршрути евакуації, доступність укриттів і невідкладної допомоги, алгоритми дій персоналу та умови безпечного відновлення роботи після реалізації загрози.

Окремим напрямом наукового забезпечення має бути вітальна безпека фахівців, які безпосередньо здійснюють запобігання терористичним загрозам, їх виявлення і припинення, а також рятувальні, вибухотехнічні, медичні та відновлювальні заходи на об’єктах критичної інфраструктури. Наукового обґрунтування потребують критерії професійного добору й готовності таких фахівців, алгоритми міжвідомчої та командної взаємодії, засоби індивідуального захисту, допустимі межі професійного ризику, порядок ротації, медико-психологічне забезпечення та відновлення після виконання завдань. Результативність відповідних заходів має оцінюватися не лише за припиненням загрози чи відновленням роботи об’єкта, а й за здатністю системи не допустити невиправданих втрат серед особового складу, рятувальників, медичних працівників, персоналу об’єкта та інших залучених фахівців.

Орієнтація на безперервність життєво важливих функцій критичної інфраструктури та мінімізацію людських втрат відповідає європейській моделі забезпечення стійкості критичних суб’єктів і безперервного надання основних послуг [12]. Застосування вітального критерію дає змогу визначати пріоритетність захисту й відновлення не за адміністративною належністю об’єкта, а за рівнем ризику виникнення незворотних наслідків для життя, здоров’я та функціональної спроможності людини.

7. Нормативна й інституційна прогалина

Порівняння встановлених наукових функцій із чинним нормативним механізмом показало, що українська система містить окремі елементи наукового забезпечення, однак вони не об’єднані в постійний дослідницький контур. Порядок проведення огляду загальнодержавної системи боротьби з тероризмом передбачає науково-методичне забезпечення відповідних процесів, а Концепція боротьби з тероризмом в Україні 2026 року орієнтує державну політику на аналіз, прогнозування, технологічний розвиток і вдосконалення спроможностей [5; 6]. Це створює нормативні передумови для використання науки, але не визначає завершеного механізму постановки дослідницьких завдань, фінансування, доступу до даних, апробації результатів та їх обов’язкового врахування.

Положення, затверджене постановою Кабінету Міністрів України № 92, визначає механізм функціонування єдиної державної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків. Аналіз його функціональної побудови не виявив окремого постійного науково-дослідного сегмента, відповідального за збирання дослідницьких потреб, координацію міждисциплінарних робіт, науково-технічну експертизу та оцінювання доказовості рішень [3]. Правила антитерористичної безпеки конкретизують вимоги до захищеності об’єктів, але також не утворюють інституції, призначеної для безперервного вироблення й упровадження нових знань [4].

Виявлена прогалина має не декларативний, а процесуальний характер. Наукові установи можуть проводити окремі дослідження, заклади освіти — готувати фахівців, а суб’єкти загальнодержавної системи боротьби з тероризмом — узагальнювати власний практичний досвід. Відокремлене функціонування зазначених елементів без їх об’єднання в єдиний скоординований цикл не забезпечує гарантованої послідовності, за якої практична проблема своєчасно трансформуватиметься в наукове завдання, дослідник отримуватиме достатні й достовірні дані, одержаний результат проходитиме контрольовану апробацію, уповноважений орган матиме визначену процедуру його впровадження, а відомості про наслідки застосування повертатимуться до науковців для перевірки й подальшого

коригування. Наявність послідовних розривів між визначенням практичної потреби, проведенням дослідження, апробацією розробленого рішення та оцінюванням результатів його впровадження дає змогу відмежувати сукупність окремих наукових робіт від цілісної системи інституціоналізованого наукового забезпечення.

8. Трирівнева інституційна модель

Для усунення встановленої прогалини запропоновано трирівневу модель, яка не підмінює чинних суб'єктів боротьби з тероризмом і не змінює їх оперативної компетенції. Її призначення полягає у створенні постійного зв'язку між стратегічним визначенням потреб, прикладним науково-аналітичним супроводом та освітньо-дослідною діяльністю.

Організаційну доцільність запропонованої трирівневої моделі пропонується оцінювати за такими критеріями: повнота охоплення дослідницького циклу, безперервність взаємодії науки і практики, чіткість розмежування функцій і повноважень, визначеність відповідальності, спроможність організувати захищену роботу з даними, ресурсна обґрунтованість та можливість незалежного оцінювання результатів. За цими критеріями необхідно порівнювати можливі способи організації наукового забезпечення: перерозподіл функцій між чинними підрозділами, міжвідомчу мережеву взаємодію, тимчасові об'єднання наукових установ і посилення наявних дослідницьких спроможностей. Перерозподіл функцій і посилення установ доцільні за наявності достатніх кадрових та організаційних ресурсів; мережева взаємодія розширює можливості залучення фахівців різних установ, але потребує постійної координації; тимчасові об'єднання придатні для виконання окремих завдань за умови збереження результатів і забезпечення наступності досліджень. Організаційна доцільність трирівневої моделі обґрунтовується поєднанням стратегічного визначення пріоритетів, постійної координації дослідницьких замовлень та розвитку наукових і освітніх спроможностей у межах єдиного циклу. Розглянуті організаційні форми можуть застосовуватися в межах цієї моделі за умови визначення їхнього місця, відповідальності та зв'язків між трьома функціональними рівнями.

Перший, стратегічний, рівень передбачає можливість створення Науково-технічної ради при Міжвідомчій координаційній комісії Антитерористичного центру при СБУ. Її доцільно визначити як колегіальний дорадчо-експертний орган, до якого залучатимуться вчені й фахівці з тероризмознавства, державної безпеки, права, психології, інформаційної та кібербезпеки, штучного інтелекту, критичної інфраструктури, вибухотехніки, біологічних і хімічних загроз, медицини катастроф та кризових комунікацій. До функцій ради пропонується віднести визначення пріоритетних напрямів досліджень, експертизу програм і технологій, розгляд результатів наукових робіт та підготовку рекомендацій щодо їх апробації. Її діяльність потребуватиме затвердженого положення, правил допуску до інформації, запобігання конфлікту інтересів і захисту інтелектуальної власності.

У разі обрання позаштатної форми діяльності ради її статус не повинен передбачати безоплатного виконання всього комплексу дослідницьких, експертних і науково-технічних робіт. Необхідно розмежовувати участь у засіданнях ради як форму дорадчої діяльності та виконання конкретних досліджень, науково-технічних експертиз або дослідно-конструкторських робіт. Фінансування доцільно спрямовувати на виконання чітко визначених завдань із установленими результатами, строками та критеріями їх приймання на договірній або програмно-цільовій основі. Запровадження диференційованого порядку участі та фінансування наукових робіт унеможливить оплату формального членства в раді й одночасно створить належні умови для залучення фахівців до виконання завдань, що потребують значних витрат часу, використання спеціального обладнання або формування окремої дослідницької групи.

Другий, координаційно-виконавчий, рівень передбачає можливість створення постійного науково-аналітичного підрозділу у структурі Штабу Антитерористичного центру при

Службі безпеки України. Розміщення такого підрозділу на виконавчому рівні зумовлене доступом Штабу Антитерористичного центру до міжвідомчої проблематики, результатів координаційної діяльності, проведених навчань та аналізу терористичних загроз. Новостворений підрозділ не повинен дублювати функції чинних оперативних та інформаційно-аналітичних структур. Основний предмет діяльності науково-аналітичного підрозділу має охоплювати формування реєстру дослідницьких потреб, підготовку технічних завдань, організацію контрольованого доступу до знеособлених даних, супроводження пілотних проєктів, наукове оцінювання одержаних результатів, а також ведення банку впроваджених рішень і вивчених уроків. Функціональне наповнення діяльності підрозділу доцільно доповнити науковим моніторингом соціально-психологічного стану суспільства, динаміки радикалізаційних ризиків, поширення страху, панічних настроїв і дезінформації, а також оцінюванням готовності різних груп населення діяти в умовах терористичної загрози.

Третій, освітньо-дослідний, рівень передбачає можливість створення у структурі Національної академії Служби безпеки України профільного навчально-наукового інституту. Функціональне призначення такого інституту полягатиме в поєднанні фундаментальних і прикладних досліджень із підготовкою фахівців, розробленням та апробацією методик. До пріоритетних напрямів його діяльності можуть належати прогнозування терористичних загроз, дослідження радикалізації, інформаційна й кібербезпека, штучний інтелект, захист критичної інфраструктури, мінімізація наслідків терористичних актів, кризові комунікації, психологія антитерористичної діяльності та вітальна безпека. Створення інституту є доцільним за умови попереднього функціонального аудиту наявних підрозділів, що дасть змогу уникнути дублювання їхніх завдань і повноважень. Інформаційну основу діяльності інституту можуть становити захищені дослідницькі бази даних, спеціалізований репозитарій наукових і методичних розробок, електронна бібліотека з питань тероризмознавства та професійна мережа дослідників і фахівців-практиків. Режим доступу до зазначених ресурсів має визначатися видом інформації, рівнем її чутливості, наявністю відповідного допуску та метою конкретного дослідження. Результативність діяльності спеціалізованого навчально-наукового осередку повинна оцінюватися не за кількістю підготовлених документів, а за часткою апробованих і впроваджених розробок, які забезпечили розв’язання конкретних практичних проблем, підвищення спроможностей системи боротьби з тероризмом або зменшення потенційних втрат для людини.

Взаємодія рівнів має відбуватися за принципом замкненого циклу. Науково-технічна рада визначає стратегічні пріоритети й оцінює значущість пропозицій; науково-аналітичний підрозділ перетворює практичні потреби на конкретні завдання та координує впровадження; навчально-науковий інститут і залучені установи здійснюють дослідження, готують методики й фахівців. Після практичної апробації результати повертаються на стратегічний рівень для оцінювання та коригування пріоритетів.

У запропонованій трирівневій моделі запобігання дублюванню функцій, бюрократизації та конфлікту компетенцій закладено в принципи її організаційної побудови. Стратегічний рівень зосереджується на визначенні дослідницьких пріоритетів і науковій експертизі, координаційно-виконавчий — на формуванні завдань та організації їх реалізації, а освітньо-дослідний — на виконанні досліджень, розробленні методик і підготовці фахівців. Такий розподіл має доповнюватися визначенням відповідального виконавця кожного завдання та меж його повноважень, що створює передумови для усунення паралельного виконання тотожних робіт і суперечностей між учасниками. Запобігання бюрократизації передбачає встановлення необхідного обсягу погоджень, строків прийняття рішень і спільного обліку дослідницьких замовлень та результатів з урахуванням режимів доступу. Попередній функціональний аудит має визначати можливості використання чинних підрозділів, а створення нових елементів — обґрунтовуватися конкретними завданнями, які не можуть бути

належно забезпечені наявними спроможностями. З огляду на передбачені механізми розмежування функцій і координації діяльності запропонована модель містить організаційні запобіжники для мінімізації зазначених ризиків, дієвість яких підлягає оцінюванню під час її пілотної апробації.

9. Доступ до даних, етичні та безпекові запобіжники

Функціонування запропонованої моделі залежить від правомірного доступу до даних. Повна відкритість операційної інформації є несумісною з охороною державної таємниці, захистом джерел, персональних даних і методів діяльності. Повна закритість, своєю чергою, унеможливлює зовнішню перевірку та обмежує якість досліджень. Для узгодження цих інтересів запропоновано багаторівневий режим наукового доступу: відкриті агреговані дані; знеособлені набори з контрольованим доступом; режимні дані для дослідників із відповідним допуском; синтетичні дані для тестування методик без розкриття реальних операційних відомостей.

Кожний дослідницький проєкт має проходити попередню правову, етичну та безпекову оцінку. Перевірці підлягають необхідність використання конкретних даних, пропорційність їх обсягу, ризик повторної ідентифікації, можливість витоку чутливої методики, вплив алгоритмічного рішення на права людини та порядок знищення або архівування матеріалів. Для проєктів із використанням ШІ необхідними є документування походження даних, контроль систематичного зміщення, тестування помилкових спрацювань, заборона повністю автоматизованого прийняття рішень із істотними правовими наслідками та можливість подальшого аудиту.

Відкриту частину наукового забезпечення доцільно реалізовувати через періодичну публікацію узагальнених оглядів загроз, пріоритетів досліджень, апробованих практик і виявлених прогалин без розголошення інформації з обмеженим доступом у відомчих наукових виданнях. Це сприятиме залученню університетів, наукових установ і технологічних компаній та дозволить уникнути паралельного фінансування тотожних розробок. Закрита частина повинна забезпечувати захищений обмін даними, проведення спеціальних досліджень і перевірку рішень у контрольованому середовищі.

10. Критерії результативності наукового забезпечення

Результативність науки у сфері боротьби з тероризмом запропоновано оцінювати за трьома взаємопов’язаними групами критеріїв. Якість наукового продукту характеризують валідність застосованої методики, відтворюваність одержаних результатів, повнота й достовірність використаних даних, чіткість установлених обмежень та готовність розробки до апробації. Практичне впровадження підлягає оцінюванню за відповідністю визначеній потребі, сумісністю з чинними процедурами, підготовленістю персоналу, ресурсною обґрунтованістю та правомірністю застосування. Досягнутий безпековий ефект визначається через фактичну зміну рівня ризику, скорочення часу виявлення загрози й реагування на неї, підвищення стійкості захищуваних функцій та зменшення потенційних втрат для людини.

Оцінювання практичного використання наукових результатів потребує розмежування факту впровадження та підтвердженої ефективності. Впровадження означає фактичне застосування розробленого методу, технології або організаційного рішення в діяльності відповідного суб’єкта; видання організаційного документа чи передання розробки замовнику саме по собі цього факту не підтверджує. Підтверджена ефективність передбачає наявність належних доказів того, що застосоване рішення забезпечує очікуваний результат за визначеними показниками та з урахуванням умов його використання. Розробка може бути впроваджена, але за результатами оцінювання виявитися недостатньо ефективною або спричиняти небажані наслідки, що становитиме підставу для її доопрацювання, обмеження чи припинення застосування. За недостатності даних ефективність слід визначати як непідтверджену, не ототожнюючи відсутність доказів із доведеною неефективністю.

Відповідно, факт застосування та його результати мають оцінюватися окремо, що відповідає доказовому підходу до перевірки контртерористичних заходів [18; 19].

Отримані результати утворюють цілісну модель, у якій випереджальна функція науки поєднується з інституційним механізмом її реалізації та вітальним критерієм оцінювання антитерористичних рішень.

Обговорення

Одержані результати дають підстави уточнити місце науки в сучасній системі боротьби з тероризмом. На відміну від підходу, за якого дослідження виконують переважно допоміжну функцію — пояснюють уже виявлені явища, узагальнюють практичний досвід або обґрунтовують окремі заходи, — у цій роботі наукове забезпечення визначено як постійний системоутворювальний цикл вироблення, перевірки та практичного застосування знань. Сформоване в дослідженні розуміння системоутворювальної ролі науки узгоджується з критичним висновком Schuurman [29] про дефіцит первинних даних, повторюваність тем і недостатню методологічну прозорість досліджень тероризму. Визначення науки як доказової основи формування та оцінювання антитерористичних рішень також розвиває висновки Lum et al. [18], які встановили обмеженість методологічно строгих оцінок ефективності контртерористичних заходів. Спільним для зіставлених наукових позицій є визнання того, що сама кількість публікацій або проведених заходів не формує достатньої доказової основи. Відмінність авторського підходу полягає в перенесенні акценту з діагностування недоліків дослідницького поля на організацію повного циклу вироблення та використання знань: від визначення практичної потреби й опрацювання операційних даних до апробації антитерористичного рішення, вимірювання його результативності та відповідного коригування державної політики.

Висновок про первинність науки має функціональний, а не адміністративний характер. Наука не підмінює повноважень Антитерористичного центру при СБУ та інших суб’єктів боротьби з тероризмом і не претендує на керівництво оперативними діями. Її первинність означає, що перед нормативним закріпленням, фінансуванням або масштабуванням рішення мають бути визначені проблема, вихідні припущення, альтернативи, допустимий ризик, очікуваний ефект і критерії перевірки. Ця інтерпретація співвідноситься з результатами Madriaza et al. [19], які виявили методологічну неоднорідність і складність установлення причинного зв’язку під час оцінювання програм запобігання насильницькому екстремізму. Mazerolle et al. [20] також констатували обмеженість доказів впливу міжвідомчих програм за участю поліції на зниження радикалізації до насильства. Причиною розбіжності між масштабом практичної діяльності та переконливістю доказів її ефективності може бути оцінювання процесуальних показників — кількості заходів, учасників або підготовлених матеріалів — замість зміни ризику та довгострокових наслідків. Запропонована модель передбачає механізм зменшення цієї розбіжності через попереднє визначення вимірюваного результату та обов’язкове оцінювання наслідків упровадження рішення.

Сформований у дослідженні цикл «операційні дані — науковий аналіз — прогноз — розроблення рішення — апробація — впровадження — оцінювання — коригування» доповнює наявні підходи до вивчення радикалізації. Wolfowicz et al. [38] довели, що фактори когнітивної та поведінкової радикалізації мають різну прогностичну значущість залежно від контексту та форми результату. Clemmow et al. [8] показали, що вразливість формується конфігурацією ризикових і захисних чинників, а не однією універсальною ознакою. Ці висновки підтверджують обґрунтовану в дослідженні необхідність застосування імовірнісного, багатофакторного та контекстуального прогнозування. Розвиваючи наведені наукові положення, запропонований цикл виходить за межі профільного аналізу та охоплює перевірку хибнопозитивних і хибнонегативних результатів, документування випадків, у яких

прогноз не підтвердився, а також повернення відомостей про наслідки практичного застосування до дослідницького масиву. Урахування зазначених результатів має принципове значення, оскільки без системного аналізу помилкових прогнозів модель може демонструвати формально високу результативність, але фактично відтворювати упередження, спричиняти стигматизацію або призводити до непропорційного втручання у права людини.

Результат щодо диференційованого доступу до операційних даних розкриває одну з причин недостатньої методологічної обґрунтованості антитерористичних досліджень. Schuurman [29] пов'язував обмеженість емпіричної основи цієї галузі з недостатнім використанням первинних джерел. Cremer et al. [9], аналізуючи кіберризики, також звернули увагу на неоднорідність, неповноту та обмежену доступність даних. У контртерористичній сфері повне відкриття інформації є неможливим через необхідність охорони державної таємниці, захисту персональних даних і джерел інформації, а також нерозголошення методів діяльності уповноважених органів. Об'єктивна необхідність забезпечення захисту інформації з обмеженим доступом не повинна призводити до звуження емпіричної основи наукових досліджень виключно до відкритих повідомлень або вторинних баз даних. Визначена в дослідженні диференціація даних на відкриті агреговані, знеособлені контрольовані, режимні та синтетичні формує збалансований механізм узгодження безпекових обмежень із вимогами наукової відтворюваності. На відміну від абстрактної вимоги щодо розширення доступу, зазначений механізм установлює для кожної категорії даних відповідну правову підставу, вимоги щодо наявності в дослідника належного допуску, порядок оцінювання ризику повторної ідентифікації та можливість проведення аудиту. Практичне значення диференційованого доступу полягає у створенні умов для перевірки наукових методик і висновків без розголошення операційної інформації з обмеженим доступом.

Подвійне використання штучного інтелекту підтверджує необхідність саме випереджальної функції науки. Lakomy [16] показав потенціал генеративних систем для масштабування пропаганди та виробництва терористичного контенту. Syllaidopoulos et al. [30] систематизували можливості застосування ШІ в контртерористичній діяльності та кібербезпеці, одночасно виокремивши етичні ризики. Wall [34] запропонував оцінювати ШІ як соціотехнічну систему, в якій дані, модель, людський контроль та наслідки помилки взаємопов'язані. Отримані в цій роботі результати загалом збігаються з такими висновками, але конкретизують їх для інституційного циклу антитерористичного рішення. Науковій перевірці мають підлягати не лише точність алгоритму, а й релевантність навчальних даних, стійкість до зміни середовища, співвідношення помилкових спрацювань і пропущених загроз, пояснюваність результату та правові наслідки його використання. Можлива причина надмірно технологічного трактування ШІ в окремих працях полягає у відокремленому аналізі програмного інструменту від організаційного середовища. Запропонований підхід розглядає його як складову системи прийняття рішень, у якій остаточна відповідальність не може бути перенесена на алгоритм.

Запропонований науково-інноваційний контур конкретизує зазначені положення, переносячи оцінювання технології з рівня її формальної новизни на рівень доведеної практичної результативності. Leszczyna [17] показав, що методи оцінювання кібербезпеки істотно відрізняються за призначенням, ресурсомісткістю та можливістю практичного застосування, тоді як Wall [34] наголосив на необхідності аналізувати технологію разом із даними, організаційними процедурами та людським контролем. На відміну від підходів, зосереджених переважно на властивостях окремого інструменту, одержані результати передбачають послідовний перехід від визначення практичної потреби до створення прототипу, його контрольованої апробації, вимірювання безпекового й вітального ефектів та повторної перевірки після зміни середовища застосування. Реалізація зазначеної

послідовності формує методологічні підстави для розмежування технологічної новизни та підтвердженої інновації, а також сприяє зниженню ризику фінансування або масштабування рішень, ефективність яких не була належним чином доведена.

Людиноцентричний результат дослідження розвиває концепцію вітальної безпеки. Ryzhov і Yashchuk [26] обґрунтували її як багатовимірну конструкцію, спрямовану на збереження життєвого потенціалу людини в умовах гібридного миру. Рижов і Ящук [27] поглибили взаємозв'язок вітальності, вітальної безпеки та життєстійкості у критичних життєвих ситуаціях. У цій статті зазначені положення перенесено в предметне поле боротьби з тероризмом і конкретизовано через вітальний критерій ефективності. Він передбачає оцінювання рішення за його здатністю запобігати загибелі й травмуванню, зберігати здоров'я, гідність, функціональну спроможність людини та доступ до життєво необхідних функцій. На відміну від традиційних відомчих показників, такий критерій не заперечує значення кількості відвернених актів, часу реагування або рівня захищеності об'єктів, але встановлює їх підпорядкованість кінцевому суспільному результату. Наукове значення цього положення полягає в концептуалізації вітальної складової антитерористичної безпеки; практичне — у можливості використовувати її для визначення пріоритетів, експертизи програм і розподілу ресурсів.

Отримані положення щодо критичної інфраструктури узгоджуються із сучасним переходом від охорони окремих об'єктів до забезпечення стійкості взаємозалежних функцій. Mottahedi et al. [21] обґрунтували необхідність поєднання технічних, організаційних і управлінських складових стійкості. Sathurshan et al. [28] встановили відсутність універсального набору показників для всіх секторів і типів загроз, а Osei-Kyei et al. [24] систематизували індикатори готовності, поглинання впливу, відновлення й адаптації. Результати цієї статті не суперечать указаним підходам, але пропонують додаткову основу їх пріоритизації — швидкість перетворення порушення функції на загрозу життю, кількість залежних від неї людей, доступність резервної послуги та час відновлення мінімально безпечного рівня. Відмінність пояснюється предметом дослідження: загальні моделі інфраструктурної стійкості вимірюють спроможність системи продовжувати функціонування, тоді як вітальна антитерористична безпека насамперед визначає, які порушення можуть спричинити незворотні наслідки для людини.

Порівняння одержаних результатів із чинними політико-правовими орієнтирами свідчить, що запропонований підхід розвиває та конкретизує їх, не підмінюючи встановлених правових механізмів. Глобальна контртерористична стратегія Організації Об'єднаних Націй поєднує запобігання тероризму, розвиток державних спроможностей і забезпечення прав людини [31; 32]. Європейський підхід до стійкості критичних суб'єктів зосереджений на забезпеченні безперервності основних послуг [12]. Концепція боротьби з тероризмом в Україні 2026 року передбачає розвиток аналізу, прогнозування, технологій і професійних спроможностей [6]. Попри закріплення зазначених стратегічних орієнтирів, ці документи не формують завершеного національного механізму, який забезпечував би безперервне перетворення практичних потреб на дослідницькі завдання, контрольований доступ до необхідних даних, організацію апробації розроблених рішень і повернення оцінених результатів у практичну діяльність. Відсутність такого постійного механізму дає підстави визначити виявлену прогалину як процесуальну, а не декларативну. На цьому ґрунтується авторська інтерпретація постанови Кабінету Міністрів України № 92: нормативний акт установлює механізм функціонування єдиної державної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, однак не виокремлює в її структурі постійного науково-дослідного сегмента [3].

Запропонована трирівнева інституційна модель є відповіддю на встановлену процесуальну розірваність. Її відмінність від моделей окремого дослідницького центру полягає у функціональному розподілі стратегічного, координаційно-виконавчого та освітньо-

дослідного рівнів. Науково-технічна рада при Міжвідомчій координаційній комісії Антитерористичного центру пропонується як дорадчо-експертний орган для визначення пріоритетів і проведення науково-технічної експертизи; постійний науково-аналітичний підрозділ Штабу Антитерористичного центру при Службі безпеки України — як механізм формування дослідницьких замовлень, організації роботи з даними, супроводження апробації та впровадження наукових результатів; профільний навчально-науковий інститут у Національній академії Служби безпеки України — як спеціалізований осередок прикладних досліджень, підготовки фахівців і перевірки методик. Зазначені елементи становлять авторську пропозицію, а не опис наявної інституційної структури. Їх створення є доцільним лише після проведення функціонального аудиту чинних підрозділів, нормативного визначення компетенції, установлення режимів доступу до інформації, правил запобігання та врегулювання конфлікту інтересів, а також джерел і механізмів фінансування. Комплексне дотримання зазначених організаційно-правових і ресурсних передумов мінімізуватиме ризики бюрократичного дублювання та зведення наукового забезпечення до формального виконання звітних процедур.

Значення трирівневої моделі полягає не у збільшенні кількості установ, а в забезпеченні постійного зворотного зв’язку між наукою і практикою. Стратегічний рівень визначає пріоритети; координаційно-виконавчий — перетворює операційні потреби на конкретні дослідницькі завдання й організовує впровадження отриманих результатів; освітньо-дослідний — створює та перевіряє рішення, одночасно забезпечуючи оновлення змісту професійної підготовки. Організаційне поєднання зазначених рівнів у межах єдиного науково-практичного циклу відповідає встановленій Borelli [7] тенденції до розширення кола учасників контртерористичного регулювання в цифровому середовищі, проте доповнює її механізмами публічно-правової підзвітності. На відміну від приватних платформ, які можуть керуватися непрозорими правилами модерації, запропоновані інституційні елементи мають функціонувати в межах нормативно визначених повноважень, установлених процедур наукової експертизи, гарантій дотримання прав людини та державного контролю.

Інтерпретація результатів потребує врахування обмежень дослідження. Запропоновані функціональна, циклічна та трирівнева моделі мають концептуальний характер і не проходили експериментальної апробації в діяльності суб’єктів боротьби з тероризмом. Висновок щодо нормативної прогалини відображає функціональний аналіз відкритих правових актів і не означає відсутності відомчих досліджень або закритих механізмів аналітичного супроводження. Оцінювання практичної результативності моделі потребуватиме пілотного впровадження, визначення базових показників, порівняння стану до і після застосування та незалежної експертизи. Окремими напрямами подальших досліджень мають стати емпірична перевірка запропонованої системи показників вітального критерію та уточнення правил їх оцінювання, розроблення протоколу доступу до знеособлених даних, визначення стандартів валідації ШІ та показників ефективності кожного інституційного рівня.

Системне зіставлення одержаних результатів із висновками сучасних досліджень підтверджує обґрунтованість переходу від епізодичного залучення науки до постійного наукового забезпечення боротьби з тероризмом. Запропонований підхід інтегрує наукові напрацювання у сферах доказовості антитерористичних заходів, дослідження радикалізації, застосування цифрових технологій, забезпечення стійкості критичної інфраструктури та дотримання прав людини в єдиний безперервний цикл вироблення, перевірки й упровадження знань. Концептуальна новизна сформованого підходу полягає в системному поєднанні трьох взаємозалежних елементів: випереджальної функції науки, інституційно забезпеченого зворотного зв’язку та вітального критерію ефективності. У межах такої моделі науковий результат набуває практичної цінності після апробації та підтвердження ефективності його впровадження, а антитерористичне рішення — людиноцентричної

спрямованості за умови його правомірності, наукової обґрунтованості та доведеної здатності знижувати загрози життю, здоров'ю, гідності й функціональній спроможності людини.

Висновки

Проведене дослідження підтвердило, що в умовах технологічної, організаційної та інформаційної трансформації тероризму наука не може залишатися допоміжним елементом антитерористичної діяльності. Її роль полягає не лише в узагальненні практичного досвіду або експертному супроводі вже ухвалених рішень, а й у завчасному пізнанні загроз, виявленні причинно-наслідкових зв'язків, побудові ймовірнісних сценаріїв, оцінюванні ризиків, розробленні та перевірці способів їх зниження. Узагальнення встановлених закономірностей дає підстави стверджувати, що наука має становити системоутворювальну, випереджальну, методологічну й доказову основу боротьби з тероризмом. Обґрунтована пріоритетність науки в системі підготовки антитерористичних рішень має функціональний, а не владно-адміністративний характер: наука не підмінює повноважень уповноважених органів, але повинна передувати нормативному закріпленню, фінансуванню та масштабуванню відповідних рішень, супроводжувати процес їх упровадження й забезпечувати перевірку отриманих результатів.

Визначено сім взаємопов'язаних функцій наукового забезпечення: пізнавальну, прогностичну, аналітичну, технологічну, експертно-оцінювальну, освітню та людиноцентричну. Їх реалізація дає змогу поєднати розвідувальні, контррозвідувальні, оперативні, правоохоронні, військові, рятувальні, інформаційні й освітні спроможності спільною доказовою основою. Відсутність хоча б однієї із цих функцій порушує цілісність системи: прогнозування без належних даних перетворюється на припущення, технологія без апробації створює додатковий ризик, а практичний результат без оцінювання залишається невідтворюваним досвідом. Взаємозалежність і безперервний характер реалізації зазначених функцій дають підстави розглядати наукове забезпечення не як сукупність епізодичних досліджень, а як постійну складову загальнодержавної системи боротьби з тероризмом.

Сформовано циклічну модель перетворення операційних даних на антитерористичне рішення: "операційні дані — науковий аналіз — прогноз — розроблення рішення — апробація — впровадження — оцінювання — коригування". Її принциповою ознакою є обов'язковий зворотний зв'язок, за якого результати практичного застосування повертаються до наукового аналізу й використовуються для перевірки вихідних припущень. До дослідницького масиву мають включатися не лише відомості про вчинені акти, а й дані про відвернені загрози, хибні сигнали, результати навчань, невдалі прогнози та рішення, які не дали очікуваного ефекту. Для узгодження потреб науки з режимними обмеженнями запропоновано диференційований доступ до відкритих агрегованих, знеособлених контрольованих, режимних і синтетичних даних із попередньою правовою, етичною та безпековою оцінкою кожного дослідницького проєкту.

Обґрунтовано науково-інноваційний контур боротьби з тероризмом, який охоплює виявлення практичної потреби, формування наукового і технічного завдання, розроблення прототипу, контрольоване випробування, правову, етичну та безпекову експертизу, пілотне застосування, оцінювання ефекту та прийняття рішення про масштабування, доопрацювання або припинення використання. Запропоновано розмежовувати експериментальну розробку, апробоване рішення і підтверджену інновацію. Сам факт придбання технології, завершення дослідно-конструкторської роботи чи видання організаційного документа не доводить її ефективності. Практична цінність інновації має підтверджуватися точністю, стійкістю, сумісністю з наявними системами, правомірністю, можливістю аудиту та вимірюваним зниженням ризику. Особливого значення ці вимоги набувають щодо штучного інтелекту, використання якого потребує перевірки якості даних, алгоритмічного зміщення, пояснюваності результатів, помилкових спрацювань і збереження реального людського контролю.

Розкрито зміст людиноцентричної парадигми вітальної антитерористичної безпеки. Встановлено, що результативність боротьби з тероризмом не може вичерпуватися кількістю проведених заходів, виявлених загроз, припинених актів або захищених об'єктів. Визначальним показником має бути реальна здатність системи запобігати загибелі й травмуванню, зберігати здоров'я, гідність, життєвий потенціал і функціональну спроможність людини. Вітальна складова антитерористичної безпеки запропонована як інтегрувальний критерій установлення пріоритетів, експертизи програм, вибору технологій, розподілу ресурсів і оцінювання наслідків. У сфері критичної інфраструктури це означає перехід від формальної захищеності окремого об'єкта до забезпечення безперервності функцій, втрата яких найшвидше створює незворотну небезпеку для життя та здоров'я населення.

Порівняння встановлених наукових функцій із нормативним механізмом України засвідчило наявність окремих передумов для наукового, аналітичного, технологічного та кадрового розвитку, але не виявило завершеного постійного науково-дослідного контуру. Зокрема, механізм, закріплений постановою Кабінету Міністрів України № 92, прямо не передбачає окремого сегмента, який забезпечував би системне формування дослідницьких завдань, координацію міждисциплінарних робіт, захищений доступ до даних, апробацію інновацій, науково-технічну експертизу та оцінювання результатів упровадження. Виявлена прогалина має процесуальний характер і не заперечує існування окремих відомчих досліджень, освітніх програм чи аналітичних напрацювань. Її зміст полягає у відсутності постійного механізму, який би об'єднував такі елементи в замкнений цикл взаємодії науки і практики.

З метою інституціоналізації наукового забезпечення боротьби з тероризмом авторами пропонується розглянути можливість формування трирівневої моделі, яка передбачатиме створення Науково-технічної ради при Міжвідомчій координаційній комісії Антитерористичного центру при СБУ, постійного науково-аналітичного підрозділу у структурі Штабу АТЦ та профільного навчально-наукового інституту в Національній академії СБУ. У межах цієї моделі стратегічний рівень визначатиме пріоритети та здійснюватиме науково-технічну експертизу; координаційно-виконавчий — перетворюватиме практичні потреби на дослідницькі завдання, організовуватиме роботу з даними, апробацію і впровадження результатів; освітньо-дослідний — поєднуватиме фундаментальні та прикладні дослідження з розробленням методик і підготовкою фахівців. Запропоновані елементи є авторською інституційною моделлю, а не описом органів, що вже функціонують.

Реалізація запропонованої моделі потребує попереднього функціонального аудиту наявних підрозділів, нормативного розмежування повноважень, установлення правил доступу до інформації, забезпечення режиму секретності, запобігання конфлікту інтересів та визначення прозорих механізмів фінансування. Науково-технічна рада може функціонувати як дорадчо-експертний орган, однак конкретні дослідницькі, експертні й дослідно-конструкторські роботи повинні оплачуватися за визначений результат, а не за формальне членство в раді. Профільний навчально-науковий інститут у Національній академії СБУ доцільно розглядати як спеціалізований осередок прикладної антитерористичної науки, що не дублюватиме діяльність наявних підрозділів, а його ефективність оцінюватиметься за практичною результативністю апробованих розробок і їхнім впливом на спроможності системи та зменшення потенційних втрат для людини.

Перспективи подальших досліджень пов'язані з подальшим розробленням та емпіричною перевіркою запропонованої системи кількісних і якісних показників вітальної складової антитерористичної безпеки; підготовкою типового протоколу доступу науковців до знеособлених операційних даних; визначенням стандартів валідації ШІ й технологій подвійного призначення; розробленням критеріїв ефективності кожного рівня запропонованої інституційної моделі. Необхідними є також експертна перевірка моделі, її

пілотна апробація на окремих дослідницьких завданнях і подальше оцінювання впливу за заздалегідь установленими показниками.

Викладені положення формують підстави для принципового переосмислення місця науки в загальнодержавній системі боротьби з тероризмом: вона повинна не наздоганяти терористичну загрозу після її прояву, а завчасно створювати знання, технології, професійні спроможності та інституційні рішення, необхідні державі для прогнозування, випередження й нейтралізації таких загроз, із визначенням збереження людського життя головним критерієм ефективності антитерористичної діяльності.

Фінансування

Дослідження виконано без залучення зовнішнього фінансування, грантової підтримки або коштів зацікавлених установ та організацій. Автори самостійно забезпечили підготовку, проведення дослідження й оформлення його результатів.

Конкуруючі інтереси

Автори заявляють про відсутність будь-якого фінансового, особистого, професійного чи іншого конфлікту інтересів, який міг би вплинути на проведення дослідження, інтерпретацію його результатів або зміст представленої наукової статті.

Використання штучного інтелекту

Під час підготовки рукопису автори використовували ChatGPT (OpenAI) як допоміжний інструмент інформаційно-аналітичного та мовностилістичного супроводу, зокрема для пошуку й систематизації тематично споріднених українських і зарубіжних досліджень, аналітичних та експертних матеріалів, а також для мовного редагування і технічної перевірки тексту. Використання системи не замінювало самостійного наукового аналізу та авторського оцінювання. Концепція і методологія дослідження, наукова аргументація, авторські положення, наукова новизна, результати, висновки та практичні пропозиції сформовані й остаточно затверджені авторами. Автори перевірили використані відомості та джерела і несуть повну відповідальність за достовірність, оригінальність та зміст рукопису. Інформація про систему: https://openai.com/chatgpt/.

Список використаних джерел

1. Про боротьбу з тероризмом : Закон України від 20 березня 2003 р. № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 06.08.2026).
2. Про критичну інфраструктуру : Закон України від 16 листопада 2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 06.08.2026).
3. Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків : постанова Кабінету Міністрів України від 18 лютого 2016 р. № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2016-%D0%BF (дата звернення: 06.08.2026).
4. Про затвердження Правил антитерористичної безпеки : постанова Кабінету Міністрів України від 15 жовтня 2024 р. № 1172. URL: https://zakon.rada.gov.ua/laws/show/1172-2024-%D0%BF (дата звернення: 06.08.2026).
5. Про Порядок проведення огляду загальнодержавної системи боротьби з тероризмом : Указ Президента України від 9 липня 2019 р. № 506/2019. URL: https://www.president.gov.ua/documents/5062019-27997 (дата звернення: 06.08.2026).
6. Про Концепцію боротьби з тероризмом в Україні : Указ Президента України від 11 червня 2026 р. № 492/2026. URL: https://zakon.rada.gov.ua/laws/show/492/2026 (дата звернення: 06.08.2026).

7. Borelli, M. (2023). Social media corporations as actors of counter-terrorism. *New Media & Society, 25*(11), 2877–2897. https://doi.org/10.1177/14614448211035121
8. Clemmow, C., Rottweiler, B., Wolfowicz, M., Bouhana, N., Marchment, Z., & Gill, P. (2024). The whole is greater than the sum of its parts: Risk and protective profiles for vulnerability to radicalization. *Justice Quarterly, 41*(1), 140–166. https://doi.org/10.1080/07418825.2023.2171902
9. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance—Issues and Practice, 47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6
10. European Parliament & Council of the European Union. (2017). Directive (EU) 2017/541 of 15 March 2017 on combating terrorism. *Official Journal of the European Union, L 88*, 6–21. https://eur-lex.europa.eu/eli/dir/2017/541/oj
11. European Parliament & Council of the European Union. (2021). Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online. *Official Journal of the European Union, L 172*, 79–109. https://eur-lex.europa.eu/eli/reg/2021/784/oj
12. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union, L 333*, 164–198. https://eur-lex.europa.eu/eli/dir/2022/2557/oj
13. Farber, S. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *Security Journal, 38*, Article 29. https://doi.org/10.1057/s41284-025-00471-7
14. Ganaie, N. A. (2026). The role of artificial intelligence in radicalisation, recruitment and terrorist propaganda: Deconstructing violent extremism and reimagining counterterrorism in contemporary digital ecosystems. *Frontiers in Political Science, 7*, Article 1718396. https://doi.org/10.3389/fpos.2025.1718396
15. Ji, A., He, R., Chen, W., & Zhang, L. (2024). Computational methodologies for critical infrastructure resilience modeling: A review. *Advanced Engineering Informatics, 62*, Article 102663. https://doi.org/10.1016/j.aei.2024.102663
16. Lakomy, M. (2023). Artificial intelligence as a terrorism enabler? Understanding the potential impact of chatbots and image generators on online terrorist activities. *Studies in Conflict & Terrorism*, 1–21. Advance online publication. https://doi.org/10.1080/1057610X.2023.2259195
17. Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security, 108*, Article 102376. https://doi.org/10.1016/j.cose.2021.102376
18. Lum, C., Kennedy, L. W., & Sherley, A. (2006). Are counter-terrorism strategies effective? The results of the Campbell systematic review on counter-terrorism evaluation research. *Journal of Experimental Criminology, 2*(4), 489–516. https://doi.org/10.1007/s11292-006-9020-y
19. Madriaza, P., Morin, D., & Hassan, G. (2025). How rigorous are evaluations of violent extremism prevention programs? Results from a systematic methodological review. *Terrorism and Political Violence*, 1–21. Advance online publication. https://doi.org/10.1080/09546553.2025.2555221
20. Mazerolle, L., Cherney, A., Eggins, E., Hine, L., & Higginson, A. (2021). Multiagency programs with police as a partner for reducing radicalisation to violence. *Campbell Systematic Reviews, 17*(2), Article e1162. https://doi.org/10.1002/cl2.1162
21. Mottahedi, A., Sereshki, F., Ataei, M., Nouri Qarahasanlou, A., & Barabadi, A. (2021). The resilience of critical infrastructure systems: A systematic literature review. *Energies, 14*(6), Article 1571. https://doi.org/10.3390/en14061571

22. North Atlantic Treaty Organization. (2024). *NATO's policy guidelines on counter-terrorism*. https://www.nato.int/cps/en/natohq/official_texts_87905.htm
23. Organisation for Economic Co-operation and Development. (2025). Ensuring the resilience of critical infrastructure. In *Government at a glance 2025*. OECD Publishing. https://www.oecd.org/en/publications/government-at-a-glance-2025_70e14c6c/full-report/ensuring-the-resilience-of-critical-infrastructure_896f59cf.html
24. Osei-Kyei, R., Almeida, L. M., Ampratwum, G., & Tam, V. (2023). Systematic review of critical infrastructure resilience indicators. *Construction Innovation, 23*(5), 1210–1231. https://doi.org/10.1108/CI-03-2021-0047
25. Python, A., Bender, A., Nandi, A. K., Hancock, P. A., Arambepola, R., Brandsch, J., & Lucas, T. C. D. (2021). Predicting non-state terrorism worldwide. *Science Advances, 7*(31), Article eabg4778. https://doi.org/10.1126/sciadv.abg4778
26. Ryzhov, I., & Yashchuk, P. (2024). Vital security: Rethinking human security in the context of hybrid peace. *Amazonia Investiga, 13*(84), 167–182. https://doi.org/10.34069/AI/2024.84.12.10
27. Рижов, І. М., & Ящук, П. В. (2026). Вітальність і вітальна безпека: Соціально-філософські засади формування життєстійкості в умовах критичних життєвих ситуацій. *Національні інтереси України, 1*(18), 358–379. https://doi.org/10.52058/3041-1793-2026-1(18)-358-379
28. Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M., & Navaratnam, S. (2022). Resilience of critical infrastructure systems: A systematic literature review of measurement frameworks. *Infrastructures, 7*(5), Article 67. https://doi.org/10.3390/infrastructures7050067
29. Schuurman, B. (2020). Research on terrorism, 2007–2016: A review of data, methods, and authorship. *Terrorism and Political Violence, 32*(5), 1011–1026. https://doi.org/10.1080/09546553.2018.1439023
30. Syllaidopoulos, I., Ntalianis, K. S., & Salmon, I. (2025). A comprehensive survey on AI in counter-terrorism and cybersecurity: Challenges and ethical dimensions. *IEEE Access, 13*, 91740–91764. https://doi.org/10.1109/ACCESS.2025.3572348
31. United Nations General Assembly. (2021). *The United Nations Global Counter-Terrorism Strategy: Seventh review (A/RES/75/291)*. https://undocs.org/A/RES/75/291
32. United Nations General Assembly. (2023). *The United Nations Global Counter-Terrorism Strategy: Eighth review (A/RES/77/298)*. https://undocs.org/A/RES/77/298
33. United Nations Interregional Crime and Justice Research Institute. (2021). *Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes*. https://unicri.it/Publications/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes
34. Wall, C. (2025). The ghost in the machine: Counterterrorism in the age of artificial intelligence. *Studies in Conflict & Terrorism*, 1–27. Advance online publication. https://doi.org/10.1080/1057610X.2025.2475850
35. Wang, Y., Zhao, O., & Zhang, L. (2024). Multiplex networks in resilience modeling of critical infrastructure systems: A systematic review. *Reliability Engineering & System Safety, 250*, Article 110300. https://doi.org/10.1016/j.ress.2024.110300
36. Weimann, G., Pack, A. T., Sulciner, R., Scheinin, J., Rapaport, G., & Diaz, D. (2024). Generating terror: The risks of generative AI exploitation. *CTC Sentinel, 17*(1), 17–24. https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation/
37. Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science, 15*, Article 100244. https://doi.org/10.1016/j.pdisas.2022.100244

38. Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2021). Cognitive and behavioral radicalization: A systematic review of the putative risk and protective factors. *Campbell Systematic Reviews, 17*(3), Article e1174. https://doi.org/10.1002/cl2.1174

References

1. Verkhovna Rada Ukrainy. (2003). *Pro borotbu z teroryzmom: Zakon Ukrainy vid 20 bereznia 2003 roku № 638-IV* [On combating terrorism: Law of Ukraine of March 20, 2003, No. 638-IV]. https://zakon.rada.gov.ua/laws/show/638-15 [in Ukrainian]
2. Verkhovna Rada Ukrainy. (2021). *Pro krytychnu infrastrukturu: Zakon Ukrainy vid 16 lystopada 2021 roku № 1882-IX* [On critical infrastructure: Law of Ukraine of November 16, 2021, No. 1882-IX]. https://zakon.rada.gov.ua/laws/show/1882-20 [in Ukrainian]
3. Kabinet Ministriv Ukrainy. (2016). *Pro zatverdzhennia Polozhennia pro yedynu derzhavnu systemu zapobihannia, reahuvannia i prypynennia terorystychnykh aktiv ta minimizatsii yikh naslidkiv: Postanova vid 18 liutoho 2016 roku № 92* [On approval of the Regulation on the unified state system for preventing, responding to and stopping terrorist acts and minimizing their consequences: Resolution of February 18, 2016, No. 92]. https://zakon.rada.gov.ua/laws/show/92-2016-%D0%BF [in Ukrainian]
4. Kabinet Ministriv Ukrainy. (2024). *Pro zatverdzhennia Pravyl antyterorystychnoi bezpeky: Postanova vid 15 zhovtnia 2024 roku № 1172* [On approval of the Rules of counter-terrorism security: Resolution of October 15, 2024, No. 1172]. https://zakon.rada.gov.ua/laws/show/1172-2024-%D0%BF [in Ukrainian]
5. Prezydent Ukrainy. (2019). *Pro Poriadok provedennia ohliadu zahalnoderzhavnoi systemy borotby z teroryzmom: Ukaz vid 9 lypnia 2019 roku № 506/2019* [On the procedure for reviewing the nationwide counter-terrorism system: Decree of July 9, 2019, No. 506/2019]. https://www.president.gov.ua/documents/5062019-27997 [in Ukrainian]
6. Prezydent Ukrainy. (2026). *Pro Kontseptsiiu borotby z teroryzmom v Ukraini: Ukaz vid 11 chervnia 2026 roku № 492/2026* [On the Concept of combating terrorism in Ukraine: Decree of June 11, 2026, No. 492/2026]. https://zakon.rada.gov.ua/laws/show/492/2026 [in Ukrainian]
7. Borelli, M. (2023). Social media corporations as actors of counter-terrorism. *New Media & Society, 25*(11), 2877–2897. https://doi.org/10.1177/14614448211035121
8. Clemmow, C., Rottweiler, B., Wolfowicz, M., Bouhana, N., Marchment, Z., & Gill, P. (2024). The whole is greater than the sum of its parts: Risk and protective profiles for vulnerability to radicalization. *Justice Quarterly, 41*(1), 140–166. https://doi.org/10.1080/07418825.2023.2171902
9. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance—Issues and Practice, 47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6
10. European Parliament & Council of the European Union. (2017). Directive (EU) 2017/541 of 15 March 2017 on combating terrorism. *Official Journal of the European Union, L 88*, 6–21. https://eur-lex.europa.eu/eli/dir/2017/541/oj
11. European Parliament & Council of the European Union. (2021). Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online. *Official Journal of the European Union, L 172*, 79–109. https://eur-lex.europa.eu/eli/reg/2021/784/oj
12. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union, L 333*, 164–198. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

13. Farber, S. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *Security Journal, 38*, Article 29. https://doi.org/10.1057/s41284-025-00471-7
14. Ganaie, N. A. (2026). The role of artificial intelligence in radicalisation, recruitment and terrorist propaganda: Deconstructing violent extremism and reimagining counterterrorism in contemporary digital ecosystems. *Frontiers in Political Science, 7*, Article 1718396. https://doi.org/10.3389/fpos.2025.1718396
15. Ji, A., He, R., Chen, W., & Zhang, L. (2024). Computational methodologies for critical infrastructure resilience modeling: A review. *Advanced Engineering Informatics, 62*, Article 102663. https://doi.org/10.1016/j.aei.2024.102663
16. Lakomy, M. (2023). Artificial intelligence as a terrorism enabler? Understanding the potential impact of chatbots and image generators on online terrorist activities. *Studies in Conflict & Terrorism*, 1–21. Advance online publication. https://doi.org/10.1080/1057610X.2023.2259195
17. Leszczyna, R. (2021). Review of cybersecurity assessment methods: Applicability perspective. *Computers & Security, 108*, Article 102376. https://doi.org/10.1016/j.cose.2021.102376
18. Lum, C., Kennedy, L. W., & Sherley, A. (2006). Are counter-terrorism strategies effective? The results of the Campbell systematic review on counter-terrorism evaluation research. *Journal of Experimental Criminology, 2*(4), 489–516. https://doi.org/10.1007/s11292-006-9020-y
19. Madriaza, P., Morin, D., & Hassan, G. (2025). How rigorous are evaluations of violent extremism prevention programs? Results from a systematic methodological review. *Terrorism and Political Violence*, 1–21. Advance online publication. https://doi.org/10.1080/09546553.2025.2555221
20. Mazerolle, L., Cherney, A., Eggins, E., Hine, L., & Higginson, A. (2021). Multiagency programs with police as a partner for reducing radicalisation to violence. *Campbell Systematic Reviews, 17*(2), Article e1162. https://doi.org/10.1002/cl2.1162
21. Mottahedi, A., Sereshki, F., Ataei, M., Nouri Qarahasanlou, A., & Barabadi, A. (2021). The resilience of critical infrastructure systems: A systematic literature review. *Energies, 14*(6), Article 1571. https://doi.org/10.3390/en14061571
22. North Atlantic Treaty Organization. (2024). *NATO's policy guidelines on counter-terrorism*. https://www.nato.int/cps/en/natohq/official_texts_87905.htm
23. Organisation for Economic Co-operation and Development. (2025). Ensuring the resilience of critical infrastructure. In *Government at a glance 2025*. OECD Publishing. https://www.oecd.org/en/publications/government-at-a-glance-2025_70e14c6c/full-report/ensuring-the-resilience-of-critical-infrastructure_896f59cf.html
24. Osei-Kyei, R., Almeida, L. M., Ampratwum, G., & Tam, V. (2023). Systematic review of critical infrastructure resilience indicators. *Construction Innovation, 23*(5), 1210–1231. https://doi.org/10.1108/CI-03-2021-0047
25. Python, A., Bender, A., Nandi, A. K., Hancock, P. A., Arambepola, R., Brandsch, J., & Lucas, T. C. D. (2021). Predicting non-state terrorism worldwide. *Science Advances, 7*(31), Article eabg4778. https://doi.org/10.1126/sciadv.abg4778
26. Ryzhov, I., & Yashchuk, P. (2024). Vital security: Rethinking human security in the context of hybrid peace. *Amazonia Investiga, 13*(84), 167–182. https://doi.org/10.34069/AI/2024.84.12.10
27. Ryzhov, I. M., & Yashchuk, P. V. (2026). Vitalnist i vitalna bezpeka: Sotsialno-filosofski zasady formuvannia zhyttiestiikosti v umovakh krytychnykh zhyttievykh sytuatsii [Vitality and vital security: Socio-philosophical foundations of resilience formation in critical life situations]. *Natsionalni interesy Ukrainy, 1*(18), 358–379. https://doi.org/10.52058/3041-1793-2026-1(18)-358-379 [in Ukrainian]

28. Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M., & Navaratnam, S. (2022). Resilience of critical infrastructure systems: A systematic literature review of measurement frameworks. *Infrastructures, 7*(5), Article 67. https://doi.org/10.3390/infrastructures7050067
29. Schuurman, B. (2020). Research on terrorism, 2007–2016: A review of data, methods, and authorship. *Terrorism and Political Violence, 32*(5), 1011–1026. https://doi.org/10.1080/09546553.2018.1439023
30. Syllaidopoulos, I., Ntalianis, K. S., & Salmon, I. (2025). A comprehensive survey on AI in counter-terrorism and cybersecurity: Challenges and ethical dimensions. *IEEE Access, 13*, 91740–91764. https://doi.org/10.1109/ACCESS.2025.3572348
31. United Nations General Assembly. (2021). *The United Nations Global Counter-Terrorism Strategy: Seventh review (A/RES/75/291)*. https://undocs.org/A/RES/75/291
32. United Nations General Assembly. (2023). *The United Nations Global Counter-Terrorism Strategy: Eighth review (A/RES/77/298)*. https://undocs.org/A/RES/77/298
33. United Nations Interregional Crime and Justice Research Institute. (2021). *Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes*. https://unicri.it/Publications/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes
34. Wall, C. (2025). The ghost in the machine: Counterterrorism in the age of artificial intelligence. *Studies in Conflict & Terrorism*, 1–27. Advance online publication. https://doi.org/10.1080/1057610X.2025.2475850
35. Wang, Y., Zhao, O., & Zhang, L. (2024). Multiplex networks in resilience modeling of critical infrastructure systems: A systematic review. *Reliability Engineering & System Safety, 250*, Article 110300. https://doi.org/10.1016/j.ress.2024.110300
36. Weimann, G., Pack, A. T., Sulciner, R., Scheinin, J., Rapaport, G., & Diaz, D. (2024). Generating terror: The risks of generative AI exploitation. *CTC Sentinel, 17*(1), 17–24. https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation/
37. Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science, 15*, Article 100244. https://doi.org/10.1016/j.pdisas.2022.100244
38. Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2021). Cognitive and behavioral radicalization: A systematic review of the putative risk and protective factors. *Campbell Systematic Reviews, 17*(3), Article e1174. https://doi.org/10.1002/cl2.1174

This is an open access journal and all published articles are licensed under a Creative Commons «Attribution» 4.0.