Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.
Державне управління: удосконалення та розвиток. 2025. № 10.

DOI: http://doi.org/10.32702/2307-2156.2025.10.3
УДК 351.862.2

А. Л. Помаза-Пономаренко,
д. держ. упр., професор, завідувач науково-дослідної лабораторії з дослідження проблем управління у сфері цивільного захисту,
Національний університет цивільного захисту України
ORCID ID: https://orcid.org/0000-0001-5666-9350
Д. В. Тарадуда,
к. т. н., доцент, професор кафедри управління діяльністю підрозділів цивільного захисту інституту післядипломної освіти,
Львівський державний університет безпеки життєдіяльності
ORCID ID: https://orcid.org/0000-0001-9167-0058

ІНСТИТУЦІЙНІ МЕХАНІЗМИ ПРОТИДІЇ ТЕРОРИСТИЧНІЙ ДІЯЛЬНОСТІ ТА ЗАБЕЗПЕЧЕННЯ СИСТЕМИ БЕЗПЕКИ

A. Pomaza-Ponomarenko,
Doctor of Sciences in Public Administration, Professor, Head of the Research Laboratory for Studying Management Problems in the Field of Civil Protection, National University of Civil Protection of Ukraine
D. Taraduda,
PhD in Technical Sciences, Associate Professor, Professor of the Department of Management of Civil Defense Units, Institute of Postgraduate Education, Lviv State University of Life Safety

INSTITUTIONAL MECHANISMS FOR COUNTERING TERRORIST ACTIVITIES AND ENSURING THE SECURITY SYSTEM

Визначено необхідність впровадження системного підходу з метою забезпечення розвитку механізмів протидії тероризму та системи безпеки. Ефективна протидія терористичній діяльності повинна функціонувати як злагоджена система з науково обґрунтованими заходами, процесами перевірки, механізмами реагування та зворотного зв'язку. Запропоновано алгоритм упровадження механізмів протидії тероризму, що (алгоритм) визначає ланцюг дій від ініціального етапу до етапу валідації та навчання. При цьому блоку «Верифікація» відведено одне з визначальних місць, що покликаний забезпечити підвищення точності рішень, з одночасним дотриманням правових норм і міжнародних стандартів. Крім того, наполягається на особливій ролі блоку навчання та попередження, що з огляду на значний таймлайн у їх реалізації потребують першочергового впровадження.

Зважаючи на комбінаторність інституційних механізмів протидії тероризму та забезпечення системи безпеки, акцентовано на важливості міжвідомчої координації як ключового чинника у підвищенні ефективності роботи цих механізмів. Інституційна співпраця між СБУ, Держспецзв'язку, ДСНС, місцевою владою та іншими зацікавленими акторами має базуватися на правових актах, SLA-протоколах і роботі координаційних центрів. Розробка централізованого аналітичного хабу для обробки інформації про потенційні загрози дозволить оптимізувати спрямування ресурсів і оперативні дії.

Окремо розглянуто питання збалансування системи безпеки та дотримання прав людини в умовах терористичних загроз. Визнано доцільність актуалізації уваги на профілактичних заходах щодо запобігання тероризму. Превентивний блок алгоритму протидії має охоплювати інструментарій боротьби з неналежним врядуванням, підвищення кібергігієни, зміцнення захисту критичної інфраструктури та ін. Наголошується на значенні спеціальної підготовки персоналу для оперативного реагування на терористичну діяльність. Регулярні навчання, симуляції надзвичайних і кризових ситуацій, перевірка відповідних протоколів дій сприяють скороченню часу прийняття рішень і вдосконаленню координації між відомствами.

The need to implement a systemic approach is identified to ensure the development of counterterrorism mechanisms and the security system. Effective counterterrorism should function as a coherent system with scientifically sound measures, verification processes, response mechanisms and feedback. An algorithm for implementing counterterrorism mechanisms is proposed, which (the algorithm) determines the chain of actions from the initial stage to the validation and training stage. At the same time, the "Verification" block is given one of the defining places, which is designed to ensure increased accuracy of decisions, while complying with legal norms and international standards. In addition, the special role of the training and warning block is emphasized, which, given the significant timeline for their implementation, require priority implementation.

Given the combinatorial nature of institutional mechanisms for countering terrorism and ensuring the security system, the importance of interdepartmental coordination as a key factor in increasing the efficiency of these mechanisms is emphasized. Institutional cooperation between the SBU, the State Service for Special Communications, the State Emergency Service, local authorities and other interested actors should be based on legal acts, SLA protocols and the work of coordination centers. The development of a centralized analytical hub for processing information about potential threats will allow optimizing the allocation of resources and operational actions.

The issue of balancing the security system and respecting human rights in the face of terrorist threats is separately considered. The feasibility of updating attention to preventive measures to prevent terrorism is recognized. The preventive block of the countermeasure algorithm should include tools for combating improper governance, improving cyber hygiene, strengthening the protection of critical infrastructure, etc. The importance of special training of personnel for an operational response to terrorist activity is emphasized. Regular training, simulations of emergency and crisis situations, and verification of relevant action protocols contribute to reducing decision-making time and improving coordination between departments.

***Ключові слова**: публічне управління, державна політика, інституційні механізми, антикризові механізми, антитерористична діяльність, виклики, терористичні загрози, кризові явища, надзвичайні ситуації, система безпеки, національна безпека, публічна безпека, цивільна безпека, інформаційна безпека, кібератаки, критична інфраструктура, органи влади.*

***Keywords:** public administration, public policy, institutional mechanisms, anti-crisis mechanisms, anti-terrorist activities, challenges, terrorist threats, crisis phenomena, emergencies, security system, national security, public security, civil security, information security, cyberattacks, critical infrastructure, authorities.*

Постановка проблеми. Важливість цього дослідження обґрунтовується потребою забезпечення системи безпеки в сучасних умовах, що неможливо реалізувати без дієвої протидії тероризму. Динаміка та характер терористичних загроз зазнають суттєвих змін під впливом регіональних конфліктів, які все частіше набувають транскордонного характеру, а також технічних інновацій і гібридних стратегій, які використовуються державними акторами. Особливого значення ця проблематика набула після 2022 року, коли рф розпочала масштабну збройну агресію проти України, що спричинило трансформацію терористичних загроз, диверсій і підривної діяльності як на національному, так і на європейському рівнях [3]. У цих умовах постала нагальна потреба оновлення підходів до протидії, що вимагає інтеграції теоретичних концепцій з емпіричними дослідженнями. Особливо це актуально для періоду з 2022 р. і до сьогодення, адже саме на основі такого поєднання можливо розробити ефективні практичні рекомендації для сфери публічного управління.

Аналіз останніх досліджень і публікацій. Науково-теоретичні засади формування безпекової політики сформували підґрунтя для досліджень як вітчизняних, так і зарубіжних учених. Серед них слід виокремити таких авторитетних дослідників В. Авер'янова, Г. Атаманчука, В. Бакуменко, П. Брауна С. Домбровську, І. Криничну, О. Крюкова, Н. Нижник, О. Кучеренко, Л. Пала, Г. Реву, Г. Ситника, В. Тертичку та ін., які зробили вагомий внесок у

розвиток теоретичних і практичних аспектів формування державної політики у сфері системи безпеки. Особливості протидії тероризму в контексті забезпечення міжнародної, національної та ін. безпеки знайшли своє відображення в роботах дослідників М. Азарова, С. Бєлая, І. Гриненко, С. Кожушко, В. Костенко, І. Кресіної, С. Кузьміна, В. Ляшенко, О. Мельник, В. Новікова, Д. Прокоф'євої-Янчиленко, О. Рибаченко, І. Хижняк та ін. [1; 2; 4].

Беручи до уваги динамічний характер змін у сфері міжнародних відносин і соціально-політичної взаємодії держав, дослідження проблематики тероризму набуває нових актуальних аспектів. Це зумовлює необхідність проведення систематичного аналізу та концептуального осмислення задля своєчасного виявлення потенційних терористичних загроз. У цьому контексті постає потреба у розробленні ефективних, аргументованих й оперативних заходів для їх нейтралізації. Аналізуючи сучасний стан наукових досліджень у цій сфері, слід наголосити, що у вітчизняній науковій традиції вивчення тероризму здебільшого орієнтоване на правові аспекти впливу терористичних дій та управлінські механізми боротьби з цим явищем. Водночас комплексний аналіз актуальних терористичних загроз в Україні та їхніх наслідків із позицій формування ефективної державної системи протидії тероризму залишається недостатньо розкритим у науковій літературі. Зокрема, це стосується розмежування терористичних дій, здійснюваних окремими організаціями, і тих, що мають ознаки державного характеру.

Постановка завдання. Метою статті є дослідження інституційних механізмів протидії терористичній діяльності в Україні в контексті забезпечення системи безпеки.

Виклад основного матеріалу. Проблема тероризму досліджується в рамках різних наукових дисциплін, зокрема політології, кримінології, соціології, правознавства та публічного управління. Комплексний підхід, розроблений у межах цих галузей, сприяє формуванню міждисциплінарної моделі дослідження, зокрема під час обґрунтування системи публічного управління та адміністрування. Вона враховує як структурні складові

(інституції, законодавство), так і функціональні аспекти (гарантування та моніторинг стану інформаційної безпеки, запобігання, реагування на її виклики тощо). Ці складники виокремлені з позиції визначення організаційно-структурного та функціонального спрямування механізмів протидії тероризму. На основі такого підходу формулюється методологія вивчення цього явища, яка включає системний аналіз, порівняльне дослідження, оцінку політик (policy analysis), зокрема аналіз неналежного управління (maladministration), кейс-стаді та статистичний огляд відкритих джерел. Для емпіричної частини роботи можуть використовуватися положення фундаментальної науки, що дозволяють представити структуру інституційних механізмів протидії тероризму (рис. 1).

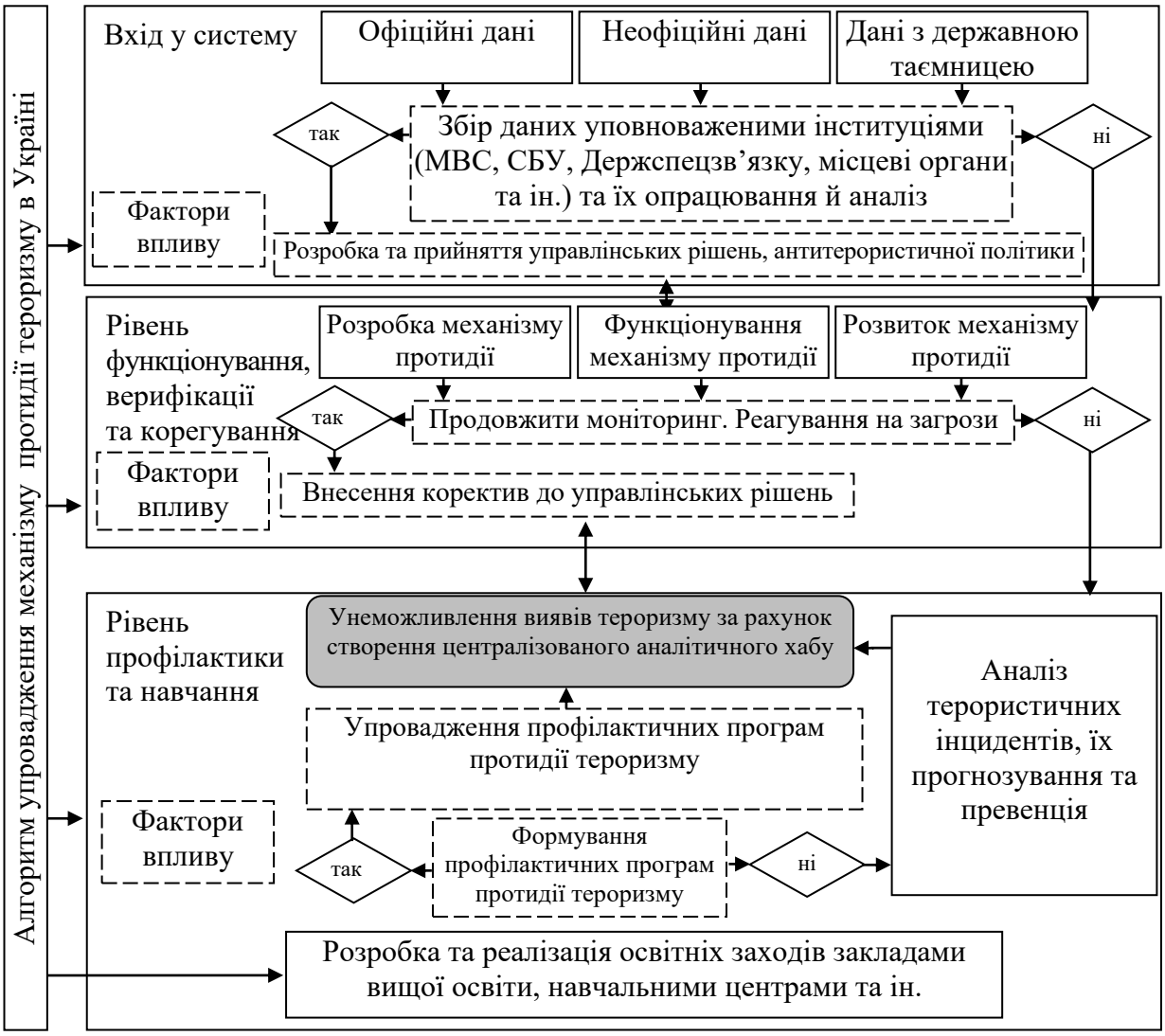

Рис. 1. Алгоритм упровадження механізму протидії тероризму та забезпечення системи безпеки в Україні

Джерело: авторська розробка.

На рис. 1 представлена інформація щодо алгоритму, який спрямований на формування комплексної системи реагування, запобігання, нейтралізації та розвитку спроможностей держави у сфері протидії терористичним загрозам. Він побудований із урахуванням принципів публічного управління та взаємодії органів сектору безпеки й оборони, а також передбачає проведення оцінювання етапів реалізації механізму протидії тероризму (табл. 1, табл. 2).

Таблиця 1. Основні етапи реалізації алгоритму протидії тероризму

Етап	Опис	Відповідальні суб'єкти	Очікуваний результат
Вхід у систему	Отримання сигналів, повідомлень, сенсорних даних про потенційну терористичну активність.	СБУ, Нацполіція, ЦОВВ у сфері безпеки	Зареєстрований сигнал для подальшої перевірки.
Збір даних	Агрегація інформації з різних джерел, систем спостереження, БД, OSINT.	Аналітичні центри, Оперативні штаби	Повна інформаційна база для аналітики.
Верифікація	Перевірка достовірності, визначення ступеня загрози, класифікація події.	Аналітичні групи, спецслужби	Встановлення істинності події (так/ні).
Оперативне реагування	Залучення сил безпеки для нейтралізації загрози, евакуації, локалізації.	ЗСУ, СБУ, ДСНС, НГУ	Ліквідація або мінімізація наслідків.
Профілактика	Аналіз інцидентів, формування профілактичних програм, освітніх заходів.	МОН, МКІП, ОМС	Зменшення ризику повторних проявів.

Джерело: авторська розробка.

Деталізований опис блоків, представлених на рис. 1, є необхідним для підвищення результативності реалізації механізму протидії тероризму

модульної системи:

1. Блок: Вхід у систему.

Мета: ініціація потоку даних / інциденту.

Вхідні дані: звернення громадян, сигнали сенсорів/камер, повідомлення СБУ/поліції, аналітичні тригери (AI/ML), дані від іноземних партнерів, телекомунікаційні / фінансові індикатори.

Дії: прийом даних у центральну платформу; маркування метаданих (час, джерело, тип); пріоритезація (критичність).

Відповідальні: оператори ЦО (аналітичний центр, Antiterror Center), служби сповіщення.

Вихід: завдання/подія у системі (ID інциденту), маршрут на збір дод. даних.

2. Блок: Збір даних

Мета: акумуляція повного набору доказів/свідчень.

Вхідні дані: запит на додаткові джерела (відео, логи, фіндані), розвіддані, соціальні мережі, ДБ.

Дії: автоматичний/ручний збір, попередня класифікація, збереження у захищеній базі.

Відповідальні: аналітики, кіберпідрозділи, оператори інфо-систем.

Вихід: повний кейс-структурований пакет даних.

3. Блок: Обробка / Аналітика

Мета: виявлення патернів, ризик-індикаторів, зв’язків.

Дії: застосування правил (rule-based), AI/ML моделей, графового аналізу, гео-прив’язки, зв’язок з переліком ризиків.

Відповідальні: аналітичні центри, SOC, NOC.

Вихід: попередній ризик-рейтинґ, рекомендація щодо переведення у статус інциденту.

4. Блок: Верифікація (так / ні) ← ключовий блок

Мета: підтвердження валідності загрози/інциденту.

Критерії верифікації:

збіг з відомими ІО (індикаторами компрометації),

кількісні порогові значення (кількість джерел, частота подій),

якісне підтвердження (свідки, відео),

підтвердження від довірених партнерів.

Процедура:

Якщо автоматичний алгоритм дає високий скор, то слід скорегувати механізм протидії на ручну перевірку.

Якщо підтверджено → (так) → Оперативне реагування.

Якщо НЕ підтверджено → (ні) → повернення в моніторинг (лог/архівація).

Відповідальні: головний аналітик, оперативний черговий, юридичний уповноважений (якщо потрібно).

Вихід (так): активний інцидент, спуск по ланцюжку реагування.

Вихід (ні): відміна інциденту або зниження пріоритету.

5. Блок: Оперативне реагування

Мета: прийняття заходів для локалізації, нейтралізації загрози.

Дії: сповіщення відповідних служб (поліція, СБУ, ЗСУ, ДСНС), розгортання сил, блокування каналів фінансування, відключення уразливих вузлів, евакуація (за потреби).

Відповідальні: командири оперативних підрозділів, центр керування кризою.

Вихід: звіти про виконані дії, першочергові результати.

6. Блок: Оцінка / Підтвердження

Мета: перевірити ефективність операції, чи загроза усунена.

Дії: пост-оперативний аналіз, перевірка відсутності повторних індикаторів, судово-експертна перевірка (за потреби).

Відповідальні: аналітичні відділи, криміналістична служба.

Вихід: статус інциденту — «закритий», «наглядається», «переактивований».

7. Блок: Профілактичні заходи

Мета: знизити ризики повторення (технічні, правові, соціальні).

Дії: посилення заходів безпеки у вразливих точках, зміни у політиці, фінансові санкції, програми деррадикалізації.

Відповідальні: міністерства, регулятори, місцева влада.

Вихід: впроваджені профілактичні заходи, оновлені процедури.

8. Блок: Навчання і тренування

Мета: підвищити навички персоналу і системну готовність.

Дії: тренування, навчання на сценаріях, міжвідомчі навчання, симуляції.

Відповідальні: навчальні центри, командування.

Вихід: оновлені процедури, сертифікований персонал.

9. Блок: Аналіз ефективності / Зворотний зв’язок

Мета: системна оцінка роботи алгоритму, оновлення моделей.

Дії: KPI-аналіз (час виявлення, час верифікації, час реагування, відсоток помилкових спрацьовувань), аудит, lessons learned.

Відповідальні: внутрішній аудитор, зовнішні експерти.

Вихід: звіт із рекомендаціями.

10. Блок: Оновлення моделей / політик

Мета: еволюція механізму протидії на основі отриманого досвіду.

Дії: дебрифінг, оновлення алгоритмів (AI/Rules), нормативних актів, SOP.

Відповідальні: науково-аналітичні центри, законодавчі ініціативи.

Вихід: впроваджені зміни, реліз нової версії механізму.

11. Блок: Розвиток системи / Масштабування

Мета: розширення охоплення, інтеграція з міжнародними партнерами.

Дії: інтеграція нових датчиків, API зв’язки з партнерами, збільшення обчислювальних ресурсів.

Відповідальні: IT-підрозділи, міжнародні відділи.

Вихід: масштабована, стійка система.

12. Блок: Архівація / Звітність

Мета: зберігання доказової бази, виконання звітних зобов’язань.

Дії: архівація кейсу, генерування звітів для керівництва, судів, партнерів.

Відповідальні: операційні центри, юридичні служби.

Вихід: архів, звіти.

Таблиця 2. Основні показники ефективності реалізації механізмів протидії тероризму та забезпечення системи безпеки

Показник	Метод оцінювання	Цільове значення
Час реагування	Моніторинг часу від сигналу до дії	≤ 5 хвилин у критичних ситуаціях
Рівень помилкових спрацювань	Порівняння підтверджених і хибних сигналів	< 10%
Кількість нейтралізованих загроз	Звіт оперативних органів	≥ 95% від виявлених
Суспільна довіра	Опитування громадян	≥ 80% позитивних відповідей

Джерело: авторська розробка.

На наше переконання, KPI / метрики ефективності системи протидії тероризму включають таке:

– Ttd (time-to-detect) — середній час від вхідного сигналу до створення кейсу (ціль < 5 хв при критичних індикаторах);

– Ttv (time-to-verify) — час від створення кейсу до рішення верифікації (ціль < 30 хв для високого ризику);

– Ttr (time-to-respond) — час від верифікації до початку реагування (ціль < 60 хв);

– % false positives — частка помилкових тривог (мета < 10%);

– % successful resolution — відсоток інцидентів, ефективно нейтралізованих (ціль > 90% для локалізованих інцидентів);

– кількість навчань/рік — мінімум 4 міжвідомчих навчання на рік.

На наш погляд, можна визначити такі технічні й організаційні рекомендації для впровадження алгоритму оцінювання стану реалізації механізму протидії тероризму:

1. Платформа: централізована платформа з модульною архітектурою (інтеграція API, плагіни для аналітики).

2. Безпека даних: шифрування в Р4, контроль доступу за ролями,

журналювання дій.

3. Юридична складова: затвердити процедури доступу до персональних даних, правила співпраці з приватним сектором (банки, провайдери).

4. Міжвідомча координація: формалізувати SLA та протоколи взаємодії (часи відповіді, формат даних).

5. Перевірка (верифікація) алгоритмів: постійне тестування AI/ML моделей на репрезентативних наборах – A/B тестування, ретроспективний аналіз.

6. Навчання: забезпечити регулярні тренування з участю юридичних, інформаційних та операційних підрозділів.

7. Міжнародна інтеграція: впроваджувати стандарти обміну даними (STIX/TAXII для кіберінформації), співпрацювати з Europol, NCTC тощо.

Приклад реалізації алгоритму оцінювання стану реалізації механізму протидії тероризму (табл. 3):

– розгорнути центральний аналітичний хаб (C2/Антитерорцентр) зі зв'язками на СБУ, МВС, ЗСУ, ДСНС;

– налаштувати джерела: CMS / SOC, фінмоніторинг банків, телеком-індикатори, соцмережі, сигнали від населення;

– налаштувати правила первинної триажної системи + AI для скорингу;

– затвердити процедури верифікації з чіткими ролями (автоматичні сценарії + ручна перевірка);

– виконувати цикли «інцидент → реагування → оцінка → оновлення» і вести журнал змін.

Таким чином, можна надати такі рекомендації для практичної імплементації інституційних механізмів протидії тероризму:

1. Запровадити централізований аналітичний хаб (на базі РНБО та у взаємодії з відповідними правоохоронними органами) для координації збору даних і керування верифікацією.

2. Уніфікувати процедури верифікації (алгоритмічні пороги + ручна експертиза) і закріпити їх нормативно з урахуванням правових гарантій.

3. Упровадити ІТ-платформу з модульною архітектурою (API-інтеграції, log/audit, AI-скори), що забезпечить кореляцію даних і одночасний доступ уповноважених служб.

4. Закласти KPI у щоквартальні звіти та проводити незалежний аудит ефективності механізму протидії тероризму.

5. Планувати регулярні міжвідомчі навчання (мінімум 4 рази на рік) та щорічний перегляд моделей поведінки загроз.

6. Удосконалити правові та фінансові інструменти для довгострокових програм превенції, модернізації технологій і підтримки операторів КІ.

7. Розвивати міжнародну взаємодію й стандарти обміну даними (STIX/TAXII, інформаційні меморандуми), особливо для кібер- і фінансових індикаторів.

Таблиця 3. Зведена таблиця «блок – відповідальний – вхід – вихід»

Блок	Відповідальний	Вхід	Вихід
Вхід у систему	Оператор ЦО	Сигнал/повідомлення	кейс_id
Збір даних	Аналітик, SOC	кейс_id, джерела	пакет даних
Обробка/Аналітика	Аналітичний центр	пакет даних	ризик-скор/рекомендації
Верифікація (так/ні)	Головний аналітик	ризик-скор	рішення (так/ні)
Оперативне реагування	Оперативні служби	рішення (так)	дії виконано
Оцінка	Аналітики	результати	статус інциденту
Профілактика	Мін/ОД(в)А/оператори	висновки	впроваджені заходи
Навчання	Навчальні центри, заклади вищої освіти	кейси	треновані кадри
Аналіз ефективності	Внутрішній аудит	KPI	оновлення політик
Оновлення моделей	Розробники/Аналітики	lessons learned	нові правила/моделі

Джерело: авторська розробка.

Запропонований алгоритм упровадження механізму протидії тероризму та наведені висновки створюють практично орієнтовану площину для побудови інституційних механізмів протидії терористичній діяльності, здатних

працювати в умовах динамічних і гібридних загроз. Реалізація цієї системи вимагатиме синхронізації правового, організаційного та технологічного рівнів, посиленого фокусу на превентивних заходах і постійного вдосконалення через навчання й оцінювання ефективності.

Висновки. На підставі проведеного аналізу можна зробити такі висновки:

1. Обґрунтована необхідність застосування системного підходу під час забезпечення розвитку механізмів протидії тероризму та системи безпеки. Визнано, що протидія терористичній діяльності повинна будуватися як цілісна система з чітко визначеними заходами, процесами верифікації, механізмами реагування та зворотного зв'язку. Запропонований алгоритм забезпечує логічну послідовність дій від «Входу в систему» до «Архівація звітності» і «Превенція/навчання», що сприяє зниженню хаотичності реагування та підвищенню оперативності управлінських рішень.

2. Визначено роль верифікації як фільтра ризику вияву терористичної діяльності. У цьому контексті запропоновано алгоритм упровадження механізму протидії тероризму, у межах якого (алгоритму) виокремлено декілька взаємопов'язаних блоків. З'ясовано, що блок «Верифікація (так/ні)» виступає критичним елементом, який мінімізує кількість помилкових спрацьовувань та забезпечує пріоритетність ресурсів для реальних загроз. Налагоджені процедури верифікації (комбінація автоматичної аналітики й ручної перевірки) підвищують достовірність прийнятих рішень і додержання правових гарантій.

3. Акцентовано, що міжвідомча координація є одним із визначальних ключів до підвищення ефективності функціонування механізму протидії тероризму. Інституційна взаємодія (СБУ, МВС, Держспецзв'язку, ДСНС, місцева влада, оператори КІ та інші зацікавлені актори) повинна бути нормативно закріплена через SLA/протоколи взаємодії й оперативні координаційні штаби. Розгляд особливостей застосування запропонованого алгоритму дозволив визначити необхідність у створенні централізованого аналітичного хабу, що координує інформацію про потенційну терористичну

небезпеку та спрямовує необхідні сили та засоби на реагування.

4. Аргументовано напрямки інтеграції технологій та аналітики. Для реалізації етапів «Збір даних» та «Обробка/Аналітика» необхідно впровадити модульні IT-платформи з можливостями AI/ML, кореляції джерел (OSINT, SIGINT, фінмоніторинг) та графового аналізу. Технології повинні працювати у поєднанні з людським контролем для уникнення алгоритмічних упереджень.

5. Баланс між безпекою та правами людини під час загрози вияву тероризму. Процедури доступу до даних, верифікації та реагування мають містити законодавчо визначені гарантії (процедури санкціонування доступу, судовий/адміністративний контроль), щоб запобігти зловживанням та зберегти суспільну довіру.

6. Конкретизовано низку превентивних заходів у межах обраної проблематики дослідження. Розділ «Профілактичні (превентивні) заходи» в алгоритмі впровадження механізму протидії тероризму має стати не другорядним, а пріоритетним напрямом: унеможливлення вияву неналежного врядування (maladministration), робота з уразливими групами, кібергігієна та посилення захисту об’єктів критичної інфраструктури та ін.

7. Окремий блок відведено навчанню, що покликано забезпечити готовність персоналу на всіх рівнях до вияву та масштабування терористичної діяльності. Регулярні міжвідомчі навчання, симуляції інцидентів і перевірки процедур зменшують час прийняття рішень і підвищують якість координації в протидії тероризму.

8. Виявлено особливості KPI і системи оцінювання ефективності. Рекомендовано запровадження показників (Ttd, Ttv, Ttr, % false positives, % successful resolution, кількість навчань/рік), що дозволяють кількісно вимірювати ефективність алгоритму впровадження механізму протидії тероризму та здійснювати його (механізму) вчасне коригування. Моніторинг KPI повинен бути регулярним і відкривати оперативний зворотний зв’язок у «Аналізі ефективності».

9. Удосконалення механізму протидії тероризму на регулярній основі

через загрозу масштабування терористичних загроз. Етапи «Аналіз ефективності / оновлення моделей / розвиток системи» у алгоритмі підкреслюють важливість адаптивності: механізмів протидії тероризму, що мають регулярно оновлюватись на основі lessons-learned, змін у загрозовому середовищі й технологічних інновацій.

10. Наполягається на міжнародній співпраці у сфері протидії тероризму та впровадженні міжнародних стандартів у цій сфері в Україні. Для підвищення можливостей і доступу до кращих практик критично важливо синхронізувати вітчизняні інституційні підходи з міжнародними стандартами (обмін інтелектуальною інформацією, STIX/TAXII, взаємодія з Europol/NCTC) та використати досвід CONTEST, DHS, FEMA тощо.

11. Підвищення організаційно-правової та фінансової стійкості інституційних механізмів протидії тероризму, що вимагає оновлення законодавчої бази та вдосконалення механізмів фінансування (державних програм, міжнародної допомоги, публічно-приватного партнерства) для реалізації довгострокових заходів щодо протидії тероризму.

12. Упровадження принципів публічності, що включає відкритість і прозорість. Підвищення рівня суспільної довіри до інституцій протидії тероризму вимагає відкритої комунікації про заходи безкомпрометації операцій: звіти, інформування громадськості, канали для зворотного зв'язку.

Література

1. Азаров М.Ю., Кузьмін С.А. Сучасний стан терористичної загрози в Україні // Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. № 2 (28). С. 43–48.

2. Гриненко І.М., Прокоф'єва-Янчиленко Д.М., Сокрут Б.В. Оцінювання та управління ризиками у сфері протидії транснаціональній організованій злочинності в Україні: кримінологічний моніторинг, тактичний аналіз та використання відкритих джерел. К.: BITE, 2015. 158 с.

3. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в

державному секторі : монографія. Харків: НУЦЗУ, 2024. 244 с.

4. Костенко В.О. Геополітичні фактори виникнення терористичних загроз та їх наслідки для України та світу // Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. 2018. Том. 29 (68). С. 218–222.

5. Помаза-Пономаренко А.Л. Глобальна безпека: “інституційна сила 4.0” // Державне управління: удосконалення та розвиток. 2024. № 11. URL: https://www.nayka.com.ua/index.php/dy/article/view/5032 (дата звернення 16.10.2025).

References

1. Azarov, M.Yu. and Kuzmin, S.A. (2012), “The current state of the terrorist threat in Ukraine”, *Borot'ba z orhanizovanoyu zlochynnistyu i koruptsiyeyu (teoriya i praktyka)*, vol. 2 (28), pp. 43–48.

2. Grinenko, I.M., Prokofeva-Yanchilenko, D.M. and Sokrut, B.V. (2015), *Otsinyuvannya ta upravlinnya ryzykamy u sferi protydiyi transnatsional'niy orhanizovaniy zlochynnosti v Ukrayini: kryminolohichnyy monitorynh, taktychnyy analiz ta vykorystannya vidkrytykh dzherel* [Risk assessment and management in the field of countering transnational organized crime in Ukraine: criminological monitoring, tactical analysis and use of open sources], VITE, Kyiv, Ukraine.

3. Dombrovska, S.M., Pomaza-Ponomarenko, A.L., Kryukov, O.I. and Poroka, S.G. (2024), *Informatsiyni zahrozy ta komunikatyvna infrastruktura v derzhavnomu sektori* [Information threats and communication infrastructure in the public sector], NUCZU, Kharkiv, Ukraine.

4. Kostenko, V.O. (2018), “Geopolitical factors of terrorist threats and their consequences for Ukraine and the world”, *Vcheni zapysky TNU imeni V.I. Vernads'koho. Seriya: Derzhavne upravlinnya*, vol. 29 (68), pp. 218–222.

5. Pomaza-Ponomarenko, A.L. (2024), “Global Security: "Institutional Power 4.0"”, *Derzhavne upravlinnya: udoskonalennya ta rozvytok*, vol. 11. available at: https://www.nayka.com.ua/index.php/dy/article/view/5032 (Accessed 13 October 2025).

Стаття надійшла до редакції 14.10.2025 р.