Прокопчук М.Л.,
здобувач освітньо-наукового рівня доктор філософії
за спеціальністю К3 «Національна безпека (за окремими сферами
забезпечення і видами діяльності)»
Науковий керівник: **Сергієнко Л.В.,**
д.н.з.держ.упр., доцент, декан факультету
національної безпеки, права та міжнародних відносин
Державний університет «Житомирська політехніка»

УПРАВЛІННЯ АНТИТЕРОРИСТИЧНОЮ БЕЗПЕКОЮ ДЕРЖАВИ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

Цифрові технології стали трансформаційним чинником у сфері антитерористичної безпеки, суттєво змінюючи як методи здійснення терористичних актів, так і підходи до їх попередження. Активне впровадження цифрових платформ, соціальних мереж, криптовалют, месенджерів та систем штучного інтелекту створює новий рівень можливостей для правоохоронних органів, але водночас надає терористичним організаціям інструменти для конспіративної діяльності, фінансування та координації атак. Особливу загрозу становить розвиток криптовалютних технологій, які забезпечують анонімність фінансових операцій та ускладнюють відстеження руху коштів, призначених для фінансування тероризму. За оцінками міжнародних експертів, обсяги використання криптовалют терористичними організаціями зростають експоненційно, створюючи нові виклики для фінансового моніторингу та міжнародної координації. В умовах цифровізації управління антитерористичною безпекою набуває критичної важливості, оскільки виникає потреба у розробці нових механізмів виявлення, запобігання та реагування на загрози, для яких характерними є високий рівень технологічності, транскордонність та складність ідентифікації.

Цифрова трансформація суспільства, попри переваги у вигляді швидкої комунікації, доступності інформації та глобальної conectivity, створює низку критичних викликів для забезпечення антитерористичної безпеки. Розширення цифрового простору та інтеграція новітніх технологій надають терористичним організаціям нові інструменти для координації, фінансування, пропаганди та вербування. За даними Глобального індексу тероризму 2024 року, використання

цифрових платформ терористичними угрупованнями зросло на 73% порівняно з 2020 роком, що демонструє стрімку адаптацію терористів до цифрового середовища. Особливу тривогу викликає використання соціальних мереж та месенджерів для радикалізації молоді – понад 60% випадків самостійної радикалізації у 2023-2024 роках відбулися через онлайн-платформи [1].

Дослідження ООН з питань боротьби з тероризмом вказують на тенденцію до цифровізації терористичної діяльності. Понад 85% терористичних організацій активно використовують зашифровані комунікації для планування атак, а 45% злочинів, пов'язаних з фінансуванням тероризму, здійснюються через криптовалюти та цифрові платіжні системи [2]. Таким чином, цифрові технології стають не лише інструментом соціального прогресу, а й засобом організації, координації та здійснення терористичних актів. Паралельно змінюється характер самих загроз – окрім традиційних форм тероризму, з'являються кібертероризм, цифрова пропаганда екстремізму, автоматизоване поширення радикального контенту та використання дронів і ШІ для підготовки атак. Такі інструменти ускладнюють виявлення загроз, а традиційні методи оперативної роботи стають недостатніми для ефективної протидії.

Сукупність цих факторів формує комплекс викликів для держави, що вимагають стратегічних рішень у сфері антитерористичної безпеки. У відповідь на зростання цифровізації терористичної діяльності дедалі важливішим стає використання передових цифрових технологій як інструментів підсилення антитерористичного потенціалу держави. Цифровізація не лише створює ризики, а й відкриває можливості для формування більш ефективної системи протидії тероризму, заснованої на превентивному підході, оперативному виявленні загроз та аналітичній підтримці рішень правоохоронних органів.

Системи на базі штучного інтелекту, машинного навчання та Big Data забезпечують постійний моніторинг цифрового простору та раннє виявлення ознак терористичної діяльності. Вони дозволяють аналізувати великі обсяги даних з соціальних мереж, форумів, месенджерів для виявлення підозрілих паттернів поведінки, радикального контенту та потенційних терористичних мереж.

В Україні Служба безпеки застосовує комплексні аналітичні системи для моніторингу цифрового середовища, що підвищує здатність держави виявляти терористичні загрози на ранніх стадіях та запобігати їх реалізації. Важливим напрямом є впровадження цифрових рішень для автоматизації аналізу загроз.

До таких інструментів належать системи розпізнавання обличчя у публічних місцях, автоматизовані платформи аналізу фінансових транзакцій для виявлення схем фінансування тероризму, технології blockchain для відстеження криптовалютних операцій та системи предиктивної аналітики для прогнозування можливих атак. Їхня інтеграція дозволяє спецслужбам значно скоротити час на обробку оперативної інформації, підвищити точність оцінювання загроз і створити комплексну картину терористичних мереж та їхньої діяльності.

Особливої уваги заслуговує міжнародна координація у сфері фінансового моніторингу та боротьби з відмиванням коштів, що використовуються для фінансування тероризму. За результатами аналізу засідання комітетів Європарламенту (ECON та LIBE) та рішення Єврокомісії, Росія потрапляє до Групи III списку високоризикованих країн (Delegated Regulation (EU) 2016/1675). Це категорія держав, які не просто мають проблеми, а становлять загрозу світовій системі. Тепер рф стоїть в одному ряду з Північною Кореєю та Іраном [3]. Таким чином, Європейська комісія активно розвиває інструменти протидії фінансовим злочинам, включаючи ведення списку високоризикових юрисдикцій, що створює додаткові бар'єри для транскордонного фінансування терористичної діяльності. Такі заходи посилюють глобальну систему фінансової безпеки та ускладнюють можливості терористичних організацій отримувати фінансування через легальні канали.

Цифрові технології відіграють ключову роль і у протидії терористичній пропаганді та радикалізації. Вони створюють інструменти для виявлення та блокування екстремістського контенту, що є важливим елементом превентивної роботи. Координаційний центр з питань протидії тероризму при СБУ використовує системи автоматизованого моніторингу онлайн-простору, алгоритми виявлення радикального контенту та технології аналізу соціальних зв'язків для ідентифікації осіб, схильних до радикалізації. Це підсилює здатність

держави своєчасно реагувати на процеси радикалізації та запобігати вербуванню громадян до терористичних організацій.

Крім того, цифрові технології сприяють удосконаленню міжнародної та міжвідомчої координації у сфері боротьби з тероризмом. Централізовані платформи обміну оперативною інформацією, автоматизовані системи Інтерполу та Європолу, стандартизовані протоколи взаємодії дозволяють правоохоронним органам різних країн швидше обмінюватися даними про підозрюваних осіб, узгоджувати спільні операції та формувати єдині бази даних терористичних загроз. Таким чином, сучасні цифрові рішення спрямовані на компенсацію ризиків, породжених цифровою трансформацією тероризму. Вони формують фундамент для побудови адаптивної, технологічно оснащеної та міжнародно інтегрованої системи управління антитерористичною безпекою держави.

Отже, впровадження цифрових технологій у сферу безпеки не лише забезпечує інноваційні можливості для протидії тероризму, а й породжує нові виклики, які суттєво впливають на управління антитерористичною безпекою держави. Актуальні глобальні тенденції свідчать, що для ефективної боротьби з сучасним тероризмом державі необхідно формувати комплексну, технологічно розвинену та міжнародно координовану систему антитерористичної безпеки, здатну відповідати темпам цифрових змін. Ефективність державної політики у сфері протидії тероризму залежить від здатності інтегрувати інноваційні цифрові рішення, забезпечити розвиток спеціалізованих компетенцій у спецслужб та сформувати адаптивну, стійку до нових форм терористичних загроз цифрову інфраструктуру безпеки.

Список використаних джерел

1. Global Terrorism Index 2024. Institute for Economics and Peace. URL: https://www.visionofhumanity.org/maps/global-terrorism-index/ (дата звернення: 01.12.2025).

2. The Use of the Internet for Terrorist Purposes. United Nations Office on Drugs and Crime. URL:

https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes.pdf (дата звернення: 01.12.2025).

3. Commission adds Russia to list of high-risk jurisdictions to strengthen international fight against financial crime. European Commission Press Corner. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2910 (дата звернення: 01.12.2025).