

УДК 343.9:343.326

БОХЕНКО В.М., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз
Служби безпеки України.
ORCID: <https://orcid.org/0000-0002-3579-4328>.

УДОСКОНАЛЕННЯ СИСТЕМИ БОРОТЬБИ З ТЕРОРИЗМОМ: ДОСВІД США

***Анотація.** Стаття присвячена аналізу системи боротьби з тероризмом у США. Наведено систему суб'єктів боротьби з тероризмом. Вказано новачі в антитерористичній діяльності правоохоронних органів та спеціальних служб США. Розглянуто окремі нормативні акти США у сфері боротьби з тероризмом. Відзначається роль громадськості у боротьбі з тероризмом, висвітлюються механізми залучення населення до цієї діяльності.*

***Ключові слова:** боротьба з тероризмом, США, національна безпека, суб'єкти боротьби з тероризмом, терористична загроза, американське законодавство.*

***Summary.** The article is devoted to the analysis of the counter-terrorism system in the United States. The system of subjects of fight against terrorism, and also innovations in anti-terrorist activity of law enforcement agencies and special services of the USA is defined. Some US regulations in the field of counter-terrorism are considered. The role of the public in the fight against terrorism is noted, the mechanisms of public involvement in this activity are highlighted.*

***Keywords:** fight against terrorism, USA, national security, subjects of fight against terrorism, terrorist threat, American legislation*

***Аннотация.** Статья посвящена анализу системы борьбы с терроризмом в США. Приведена система субъектов борьбы с терроризмом. Указаны новации в антитеррористической деятельности правоохранительных органов и специальных служб США. Рассмотрены отдельные нормативные акты США в сфере борьбы с терроризмом. Отмечается роль общественности в борьбе с терроризмом, освещаются механизмы привлечения населения к этой деятельности.*

***Ключевые слова:** борьба с терроризмом, США, национальная безопасность, субъекты борьбы с терроризмом, террористическая угроза, американское законодательство.*

Постановка проблеми. Сьогодні боротьба з тероризмом є одним з найбільш проблемних питань міжнародної безпеки, глобальної взаємодії та співпраці. Сучасний тероризм давно вже став явищем інтернаціональним, транскордонним, глобальним, й таким, що загрожує не тільки окремим державам, а й міжнародній безпеці в цілому. В цьому плані цікавим є американський досвід протидії тероризму, оскільки в США створено власну масштабну загальнодержавну систему виявлення, запобігання і припинення терористичної діяльності. Спецслужби та правоохоронні органи США активно взаємодіють з цією метою з спеціальними службами інших країн, проводять активні операції за кордоном. В лютому 2015 року відповідні служби США підписали дві нових угоди з Європолом щодо протидії нелегальній міграції та іноземним бойовикам. Це забезпечило платформу для обміну інформацією щодо осіб, які забезпечують вербування та переправлення іноземних бойовиків, а також джерел їх фінансування [1]. У результаті цієї діяльності рівень терористичної загрози порівняно з країнам Європи понизився. Водночас, на думку американських аналітиків, у 2020 – 2021 рр. терористична загроза у США значно зросте через декілька факторів: президентські вибори та реакцію на кризу, пов'язану з поширенням інфекційної хвороби CoVID-19 [2, с. 380].

Крім цього, посилення міграційних процесів створює додаткові можливості для активізації діяльності міжнародних терористичних організацій. З огляду на це, США вживають заходів щодо посилення прикордонного контролю, впровадження ефективних систем спостереження за мігрантами, запобігання нелегальній міграції, як важливих елементів системи попередження вчинення терористичних актів [1].

Результати аналізу наукових публікацій. Дослідженням досвіду боротьби з тероризмом займалися багато вчених: Б. Дженкінс, Г. Деникер, [3], В. Лакер [4], Р. Паркес [5], Р. Хантер, А. Шмід [6] та ін. Серед українських дослідників слід виділити праці В.Ф. Антипенка [7], В.П. Ємельянова [8], Б.Д. Леонова [9], В.В. Мокляка [10], А.В. Савченка, О.Г. Семенюка, О.В. Шамари та ін. Найбільш актуальним і дієвим, на нашу думку, є досвід США, де існує стабільна правова система, а правова діяльність у цій країні має вагому базу напрацювань у сфері запобігання терористичним актам.

Метою статті є оцінка сучасних тенденцій розвитку антитерористичної діяльності у США в контексті запозичення позитивного зарубіжного досвіду під час удосконалення державної політики у сфері боротьби з тероризмом в Україні.

Виклад основного матеріалу. Аналіз боротьби з тероризмом в США умовно можна поділити на два періоди: до 11.09.2001 р. і після цієї дати. Жахливі теракти 11 вересня 2001 року в США змінили свідомість американського суспільства, в тому числі його ставлення до терористичної загрози. Ці події призвели до активізації антитерористичної діяльності в США та за її межами, зокрема, під час здійснення воєнних операцій в Іраці та Афганістані.

З метою підвищення ефективності боротьби з міжнародними терористичними організаціями, а також координації діяльності різних суб'єктів боротьби з тероризмом були розроблені низку нормативно-правових актів. Вже у жовтні 2001 року був прийнятий Федеральний Закон “Патріотичний акт” (USA PATRIOT Act) [11], який істотно розширив можливості правоохоронних органів, спеціальних служб та органів національної безпеки у сфері запобігання тероризму з виявлення і попередження терористичних актів, що готуються як на території США, так і за кордоном. Вони визначили новий, більш системний підхід до протидії тероризму в XXI столітті [2, с. 72].

З моменту прийняття “Патріотичного акта” в американському суспільстві розпочалася критика багатьох його положень, а особливо тих, що стосувалися розширення процедури таємного нагляду за особами, що підозрюються у терористичній діяльності [10, с. 220]. Відтепер правоохоронним органам та спеціальним службам дозволялось: розкривати один одному службову й “таємну” інформацію, що тим чи іншим чином стосувалася кримінального переслідування осіб, що підозрюються у тероризмі; спостереження, тобто таке прослуховування за допомогою електронних засобів, коли воно проводиться не відносно конкретно зафіксованого номера телефону, а щодо розмов об'єкта спостереження з усіх телефонних апаратів при його пересуванні (розділ 206 Акта). Окрім цього, були розширені можливості електронного спостереження за підозрюваними у тероризмі: збільшено перелік даних, які повинен надавати провайдер на запит правоохоронних органів (підрозділи 209 – 212, 217 Акта); наділено юридичним імунітетом провайдерів та інші організації, що надають допомогу у розслідуванні, стосовно розголошених у зв'язку із цим даних (підрозділ 225 Акта); спрощена офіційна процедура застосування спеціальних пристроїв для негласного збору інформації у комп'ютерних мережах (підрозділ 216 Акта) [10, с. 220; 11].

За результатами антитерористичної реформи було створено або реорганізовано понад 263 державні установи для реалізації антитерористичної діяльності [12]. Проте,

реалізація ефективної стратегії боротьби зі злочинністю – справа, якою займалися всі держави не одне століття, помітних здобутків так і не досягла [3, с. 76-77].

Відповідно до Акта про національну безпеку від 25 листопада 2002 р. створено Міністерство національної безпеки США, яке об'єднало 22 федеральних відомства та агентства, а також Адміністрацію транспортної безпеки США [13]. Серед завдань Міністерства національної безпеки США варто відзначити: запобігання терористичній діяльності та транснаціональній злочинності; забезпечення безпеки кордонів; реалізацію імміграційної та митної політики; забезпечення економічної безпеки та кібербезпеки; запобігання стихійним лихам та іншим надзвичайним ситуаціям [14].

Крім Збройних Сил, до складу системи суб'єктів запобігання тероризму США також входять консультативні органи при президентові США для координації діяльності суб'єктів боротьби з тероризмом та вирішення проблем національної безпеки із зовнішньої політики та внутрішньої безпеки, серед яких виділяється Рада національної безпеки США, Рада внутрішньої безпеки США [15], Національний координатор з безпеки, захисту інфраструктури та боротьби з тероризмом та ін. [10, с. 223-224]. Важливе місце у системі боротьби з тероризмом займає Федеральне бюро розслідувань та Центр з відстеження терористичної активності.

ФБР наділене широким колом повноважень, достатнім матеріально-технічним забезпеченням, великим штатом професійних агентів, значним надбанням у розвідувальній і оперативній діяльності, завдяки цьому їм вдається якісно та рішучо попереджати терористичні акти у великих містах США. Співробітники ФБР значну увагу приділяють просвітницькій і профілактичній діяльності серед населення, застерігаючи людей захищати себе як у мережі, так і при особистій зустрічі, а також закликають одразу ж повідомляти про будь-яку підозрілу активність, із якою вони стикаються [2, с. 383].

Помітну роль у боротьбі з тероризмом відіграє Центральне розвідувальне управління, яке займається зовнішньою розвідкою терористичних загроз. При ЦРУ функціонує спеціальний підрозділ – Антитерористичний центр, який збирає інформацію про терористичні об'єднання в усьому світі. Спеціалісти цього підрозділу беруть участь у підготовці щорічних звітів про стан тероризму в світі [10, с. 225].

У США діє Національний контртерористичний центр, до завдань якого віднесено проведення міжвідомчих засідань щодо виявлення внутрішніх і зовнішніх загроз інтересам держави; аналітична діяльність і вироблення рішень з протидії тероризму, надання інформації щодо світової розробки інноваційних рішень у сфері боротьби з тероризмом. Також існує інформаційний центр вивчення тероризму ім. Меіра Аміта, метою діяльності якого є акумуляція, дослідження та розповсюдження інформації стосовно тероризму та розвідувальної діяльності.

Наприкінці 2018 р. Президент США затвердив Національну стратегію боротьби з тероризмом, яка втілює в собі новий еволюційний підхід у процесі стабілізації рівня терористичних актів і знешкодження терористичної загрози в усьому світі та на теренах Америки. Ця стратегія відрізняється від попередніх тим, що вона застосовує більш рухливий та експансивний підхід, який розглядає весь спектр терористичних загроз для США, включаючи зарубіжних ворогів та осіб, на яких вони прагнуть впливати та яких планують вербувати для вчинення насильства у США [2, с. 380]. Тобто центральна мета стратегії спрямована на захист американських свобод і непохитність у зобов'язанні перемогти всіх, хто застосовує насильство, намагаючись знищити, дестабілізувати чи погіршити стан суспільства [16; 2].

Основні цілі та задачі США у процесі запобігання терористичним актам, спрямовані на: зменшення рівня нападів терористів на території штатів; знищення фінансових,

матеріальних і матеріально-технічних джерел сили та підтримки терористів; ліквідацію спроможності терористів вербувати людей і надихати на реалізацію терористичних цілей; посилення охорони кордонів; покращення діяльності правоохоронних органів; протидію придбання терористами та використання ними зброї масового ураження; розширення кола партнерів із державного та приватного сектору, в т.ч. іноземних [17].

У процесі розробки та реалізації заходів запобігання терористичним актам у США опираються на три принципи, серед яких активне партнерство; масштабність, гнучкість та адаптованість; готовність діяти [2, с. 380; 18].

Не останню роль у боротьбі з тероризмом відіграють інформаційні технології без яких неможливо уявити сучасне суспільство. У зв'язку з сутнісними відмінностями сучасних інтелектуально насичених технологій ведення війни від традиційних, для ефективного функціонування системи антитерористичного захисту необхідно змінювати принципи і моделі антитерористичної діяльності, формувати інноваційно-креативне мислення, нові концепції, теорії, методи та технології інноваційного розвитку [19]. Основне завдання подібних технологій зводиться до розпізнавання, формалізації та оцінки загроз терористичного характеру для прогнозування терористичної активності.

Найбільшою перевагою застосування інформаційних технологій є швидкість, з якою адресат отримує інформацію, що має значення для розкриття кіберзлочинів. Цим скористалася компанія Palantir Technologies, послугами якої користуються ЦРУ, ФБР, Міноборони США, Військово-повітряні сили США, Корпус морської піхоти США, командування спеціальних операцій, Військова академія США. Інформаційна система Palantir аналізує інформацію про колишні правопорушення підозрюваних злочину, їх родичів та оточення, автомобільні номери та іншу супутню інформацію, яка прямо або опосередковано стосується підозрюваного [20].

Окремо слід виділити державну програму США з негласного збору інформації, яка передається каналами електрозв'язку – PRISM. Лише у 2010 році завдяки PRISM було перехоплено та зібрано близько 1,7 млрд. телефонних перемовин та електронних повідомлень, а також близько 5 млрд. геолокаційної точок місцезнаходження власників мобільної техніки. Як тільки особа, що несе інтерес з боку органів поліції або держбезпеки, потрапляє до бази даних Palantir, інформація про неї відразу розповсюджується відповідним співробітникам. Слідчі мають можливість отримувати повідомлення про осіб, які підпадають під завчасно визначені параметри пошуку: раса, стать, вік, зріст тощо. У штатному режимі працівники спецслужб вносять до бази даних інформацію про особу, яка причетна до тероризму [21]. Також Palantir реалізовано систему виставлення рейтингових балів залежно від ступеня небезпеки, яку несе особа, кількості скоєних правопорушень, затримань органами поліції тощо. Співробітникам спецслужб достатньо кількох хвилин, щоб мати уявлення про пряму чи опосередковану причетність осіб до терористичної діяльності [22].

Зацікавленість викликає ще один напрямок боротьби з тероризмом, який з'явився у США з огляду на особливості терористичної атаки у 2016 р. у м. Ніцца (Франція), де зловмисником використовувалась вантажівка. Передбачається, що у США до 2021 року до Інтернету речей буде приєднано близько 250 млн. транспортних засобів, управління якими може здійснюватися через Інтернет. Це надає терористам можливість перехоплювати управління такими засобами та вчиняти терористичні атаки дистанційно, навіть не перетинаючи державний кордон. З огляду на таку потенційну загрозу в Міністерстві юстиції США розпочала функціонувати окрема група, що опікується виключно питаннями Інтернету речей [1].

Особливим відділом ФБР по боротьбі з тероризмом було підготовлено та представлено на своєму сайті матеріал, присвячений мінімальним запобіжним заходам: громадянам пропонується ознайомитися з інформацією про місця підвищеної небезпеки, про рекомендовані дії у разі виявлення сумнівних пакетів і згорток на вулицях, у транспорті, в інших публічних місцях. На сайті містяться відомості щодо офіційної оцінки рівня терористичної загрози в конкретний момент, а також своєрідний “інструктаж” для тих, хто планує закордонні поїздки в “небезпечні” зони [23].

Важливе значення у сфері протидії тероризму має реалізація спеціальних програм та ініціатив під егідою Державного департаменту США. У Департаменті функціонує Бюро з протидії тероризму та насильницькому екстремізму, що займається розробкою скоординованих стратегій та підходів до боротьби з тероризмом за кордоном та забезпечує антитерористичне співробітництво міжнародних партнерів. Серед інших обов'язків Бюро реалізує такі програми та ініціативи: Програма допомоги у боротьбі з тероризмом, Програма протидії насильницькому екстремізму, Програма протидії фінансуванню тероризму, Фонд боротьби з тероризмом та багато ін. [24]. Також важливими аспектом антитерористичної діяльності в США є залучення громадськості до боротьби з тероризмом, яке надає допомогу правоохоронним органам для підтримання правопорядку.

Отже, система запобігання терористичним актам у США характеризується вагомою законодавчою базою, яка повністю забезпечує функціонування державних органів у цій сфері; широким спектром суб'єктів запобігання терористичним актам у великих містах, діяльність яких оперативна та скоординована між собою; активною участю фізичних осіб, громадських організацій, релігійних спільнот і представників приватної діяльності у попередженні злочинних намірів терористів; розгалуженою низкою заходів, серед яких – захист кордонів, захист уразливих об'єктів інфраструктури, викриття спроб вербування людей терористами у терористичну діяльність, мінімізація терористичної пропаганди через ЗМІ та Інтернет, міжнародне співробітництво та формування соціальної стійкості до терористичного акту [2, с. 384].

Висновки.

Дослідження досвіду США є важливим завданням суб'єктів боротьби з тероризмом в контексті удосконалення вітчизняної антитерористичної діяльності. В США існує розгалужена державна система боротьби з тероризмом, основу якої утворює значна кількість суб'єктів боротьби з тероризмом. Важливе значення має використання інформаційних технологій під час взаємодії таких суб'єктів, що значно підвищує ефективність обміну інформацією між ними. Важливу роль у цій діяльності відіграють громадські організації, які активно співпрацюють з правоохоронними органами у напрямі запобігання тероризму. Активне залучення громадян і суспільства в цілому до боротьби з цим небезпечним явищем дозволить підвищити ефективність такої діяльності і рівень довіри населення до відповідних уповноважених органів [1].

Використана література

1. Актуальні питання протидії тероризму у світі та в Україні: аналіт. доп. / Резнікова О.О., Місюра А.О., Дрьомов С.В., Войтовський К.Є.; за заг. ред. О.О. Резнікової. Київ: НІСД, 2017. 60 с.
2. Стукаліна О.В., Кулик Л.М. Міжнародний досвід запобігання терористичним актам у великих містах. URL: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/84/2184/4720-1?inline=1> (дата звернення: 13.06.2021).
3. Деникер Г. Стратегия антитеррора: факты, выборы, требования. Новые пути борьбы с терроризмом. Терроризм в современном капиталистическом обществе. Москва, 1982. Вып. 2. С. 76-80.

4. Laqueur W. Postmodern Terrorism. *Foreign Affairs*. Vol. 75. № 5 (Sept./Oct.). 1996. P. 24-36.
5. Parkes R. Migration and terrorism: the new frontiers for European solidarity. European Union Institute for Security Studies, Brief Issue 37, December 2015. 4 pp.
6. Schmid A.P., Tennes J. Terrorism and Migration: An Exploration. The Hague: International Centre for Counter Terrorism (ICCT), 2016. 63 pp.
7. Антипенко, В.Ф. Оптимізація антитерористичної системи держави в умовах міжнародної і регіональної інтеграції. Київ, 2008. 406 с.
8. Емельянов В.П. Терроризм и преступления с признаками терроризирования (уголовно-правовое исследование): монография. Москва: Nota Bene, 2000. 320 с.
9. Леонов Б.Д. Запобігання тероризму: кримінологічний аспект: монографія. Київ: Видавничий дім "АртЕк". 2015. 435 с.
10. Мокляк В.В. Сучасний досвід США у сфері запобігання тероризму. *Питання боротьби зі злочинністю*. 2017. № 34. С. 219-229. URL: http://nbuv.gov.ua/UJRN/Pbzz_2017_34_20
11. Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 / Public Law 107-56 – OCT. 26, 2001. URL: <https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf> (дата звернення: 12.06.2021).
12. Green, Shannon N. Do we need a new strategy to prevent terrorist attacks on the United States? Center for strategic and international studies. URL: <https://www.csis.org/analysis/do-we-need-new-strategy-prevent-terrorist-attacks-united-states> (дата звернення: 09.06.2021).
13. Homeland Security Act of 2002. Public Law 107–296. URL: <https://legcounsel.house.gov/Comps/Homeland%20Security%20Act%20of%202002.pdf> (дата звернення: 13.06.2021).
14. Our Mission – Department of Homeland Security. URL: <https://www.dhs.gov/our-mission> (дата звернення: 13.06.2021).
15. Homeland Security Presidential Directive-1. October 29, 2001. URL: <https://fas.org/irp/offdocs/nspd/hspd-1.htm> (дата звернення: 13.06.2021).
16. National Strategy for Counterterrorism of the United States of America. URL: <https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf> (дата звернення: 09.06.2021).
17. National Prevention Framework. Second Edition. URL: https://www.fema.gov/media-librarydata/146601720927983b/72d5959787995794c08/74095500b1/National_Prevention_Framework_2nd.pdf (дата звернення: 10.06.2021).
18. URL: https://www.fema.gov/medialibrarydata/146601720927983b/72d5959787995794c08/74095500b1/National_Prevention72d5959787995794c08/74095500b1/National_Prevention_Framework_2nd.pdf (дата звернення: 10.06.2021).
19. Блэкнер Ф. Информационные технологии и организации: уроки 80-х и перспективы 90-х. (Психология труда и организационная психология). Москва, 1995. 448 с.
20. Офіційний сайт Palantir. URL <https://www.palantir.com> (дата звернення: 12.06.2021).
21. PRISM (программа разведки). URL: [https://ru.wikipedia.org/wiki/PRISM_\(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0_%D1%80%D0%B0%D0%B7%D0%B2%D0%B5%D0%B4%D0%BA%D0%B8\)](https://ru.wikipedia.org/wiki/PRISM_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0_%D1%80%D0%B0%D0%B7%D0%B2%D0%B5%D0%B4%D0%BA%D0%B8)) (дата звернення: 12.06.2021).
22. Terrorist Threat integration. URL: <https://www.dni.gov/index.php/nctc-who-we-are/history>
23. Safety and Security for the Business Professional Abroad. URL: <https://www.fbi.gov/file-repository/business-travel-brochure.pdf/view>(дата звернення: 12.06.2021).
24. Programs and Initiatives – U.S. Department of State. URL: <https://www.state.gov/j/ct/programs/index.htm#ISEG> (дата звернення: 12.06.2021).

~~~~~ \* \* \* ~~~~~