УДК 351.86:[004:343.326](100-87:477)
DOI https://doi.org/10.32836/2310-9653-2020-1.18

О. І. Жайворонок, аспірант
кафедри глобалістики, євроінтеграції та управління
національною безпекою Національної академії
державного управління при Президентові України

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ ТА ЙОГО ІМПЛЕМЕНТАЦІЯ В УКРАЇНІ

У науковій статті досліджено практичні підходи до боротьби з інформаційним тероризмом у системі міжнародного законодавства та міжнародних і національних інституцій провідних країн світу. Виявлено, що всеосяжного міжнародного документа з питань боротьби з інформаційним тероризмом, який був би спеціально спрямований на запобігання і припинення використання телекомунікаційних технологій терористами, поки немає. До того ж міжнародне співтовариство досі не дійшло згоди щодо утвердження на міжнародному рівні єдиного визначення терміна «тероризм».

Розглянуто досвід провідних європейських і світових країн, яких торкнулася хвиля терактів, що працюють над модернізацією свого антитерористичного законодавства, включно з нормами, що регулюють механізми збору даних (відеоспостереження, прослуховування, реєстрація і передача даних про неповнолітніх і т.д.). Встановлено, що в багатьох випадках законопроєкти були далеко не новими і протягом тривалого часу вони безуспішно лобіювались національними органами безпеки, натикаючись на великий опір у парламенті, і були прийняті тільки після терактів. Зроблено висновок, що найефективнішим у довгостроковій перспективі заходом протидії тероризму в Європі експерти вважають боротьбу з пропагандою радикального ісламу.

При цьому зусилля Європейських країн сьогодні спрямовані (окрім стандартних, але, безсумнівно, необхідних, методів боротьби з тероризмом – підготовки спецпідрозділів, що задіюються до антитерористичних заходів) на підвищення рівня боротьби з кібертероризмом і пропагандою тероризму, що являють собою ключові складники боротьби з інформаційним тероризмом. А якщо трансформувати конкретний досвід європейських спецслужб щодо протидії Ісламській державі на ситуацію, що складається навколо вітчизняного інтернет-простору, зокрема пропаганди російських спецслужб, формування народних думок навколо ситуації на сході країни, то підходи до боротьби з інформаційним тероризмом Європейських країн, на нашу думку, було б непогано застосовувати вітчизняними підрозділами боротьби з інформаційним тероризмом. При цьому слід зауважити, що системний підхід у зазначеному напрямі в Європі сьогодні ще не сформовано.

Проведено порівняльний аналіз норм міжнародного права у сфері протидії інформаційному тероризму з метою його практичного застосування в Україні.

Зроблено висновок про те, що публічне управління у сфері протидії інформаційному тероризму може бути ефективним лише за умови тісної співпраці державних органів і громадських організацій, об'єднань та окремих громадян.

Ключові слова: *тероризм, інформаційний тероризм, кібертероризм, міжнародне співтовариство, протидія інформаційному тероризму.*

O. I. Zhaivoronok. International experience against information terrorism and its implementation in Ukraine

Practical approaches to combating information terrorism in the system of international law and international and national institutions of the leading countries of the world are explored in the scientific article. It is revealed that a comprehensive international document on combating information terrorism specifically aimed at preventing and stopping the use of telecommunications technologies by terrorists does not yet exist. In addition, the international community has so far not agreed on the adoption at international level of a single definition of the term "terrorism".

The experience of leading European and world countries affected by the wave of terrorist attacks working on the modernization of their anti-terrorist legislation, including rules governing data collection mechanisms (video surveillance, listening, recording and transmission of data on minors, etc.), is considered. It was found that in many cases the bills were far from new and for a long time they were unsuccessfully lobbied by national security agencies, meeting with great resistance in parliament and were adopted only after the terrorist attacks. It is concluded that the most effective long-term counterterrorism measure in Europe is that experts believe that the fight against radical Islam is being promoted.

At the same time, efforts of the European countries today are directed (in addition to standard, but undoubtedly necessary, methods of counter-terrorism – preparation of special units engaged in anti-terrorist activities) to increase the level of combating cyber terrorism and the promotion of terrorism, which is a key component of counter-terrorism. And if we transform the specific experience of the European intelligence services, in counteracting the Islamic State to the situation around the domestic Internet space, including the propaganda of Russian intelligence services, forming popular thoughts around the situation in the East of the country, then approaches to combat information terrorism in European countries it would be a good idea to use domestic counter-terrorism units. However, it should be noted that a systematic approach in this direction in Europe has not yet been established.

A comparative analysis of international law norms in the field of combating information terrorism has been conducted with a view to its practical application in Ukraine.

It is concluded that public administration in the field of combating information terrorism can be effective only if close cooperation between state bodies and public organizations, associations and individual citizens.

Key words: *terrorism, information terrorism, cyberterrorism, international community, counteraction to information terrorism.*

Постановка проблеми. Практичні заходи з боротьби з інформаційним тероризмом потребують ефективного функціонування національних організаційно-правових механізмів боротьби з цим злочинним явищем у тісній взаємодії зі скоординованими діями міжнародної спільноти, а також врахування, ратифікації та імплементації міжнародних правових актів, досвіду і практики провідних країн світу. Аналіз останніх допоможе окреслити ефективні шляхи не тільки застосування, а й реформування, модернізації вітчизняної антитерористичної системи у сфері протидії інформаційному тероризму.

Аналіз останніх досліджень і публікацій. Аналіз стану наукової розробленості проблеми нормативно-правового і практичного забезпечення протидії інформаційному тероризму в Україні із застосуванням міжнародного досвіду та підходів до цього питання у національних інституціях провідних країн світу вказує на безсумнівно велику кількість наукових досліджень із цієї тематики. У своїй праці «Інформаційна безпека України в умовах євроінтеграції» В. Ліпкан, Ю. Максименко, В. Желіховський доходять висновку, що інформаційний тероризм застосовується з метою дезінформації, дезорієнтації і профанації для помилкового сприймання, помилкового розуміння і неадекватної поведінки суспільства [1, с. 15]. А. Катренко у своїй роботі «Особливості інформаційної безпеки за міжнародними стандартами», розглядаючи Резолюцію Генеральної Асамблеї ООН № 53/70 з кіберзлочинності, прийняту у грудні 1998 року, справедливо наголошує, що держави-члени повинні інформувати Генерального секретаря ООН про свої погляди і оцінки щодо проблем інформаційної безпеки, визначення основних понять, пов'язаних з інформаційною безпекою і розвитком міжнародних принципів, що поліпшують глобальний інформаційний простір і телекомунікації та допомагають боротися з інформаційним тероризмом [2, с. 15–17].

Свої погляди на вітчизняну систему інформаційної безпеки розкриває Ю. Радковець «Погляди на створення системи інформаційної безпеки України та її Збройних Сил». У своїй роботі автор розглядає системи інформаційної безпеки США, Великої Британії, Ізраїлю, Китаю, Польщі, Болгарії, Румунії, Словаччини, Угорщини, Чехії та інших країн світу, робить їх аналіз і уможливлює практичне застосування в Україні з метою підвищення ефективності функціонування вітчизняної системи боротьби з інформаційним тероризмом через призму реальних кібернетичних загроз для об'єктів критичної інфраструктури цих країн [3, с. 38–42].

Водночас підходи до проблем інформаційного тероризму у світових країнах, а також у міжнародних інституціях різні, форми залучення і методи співпраці урядових організацій і громадськості теж різні, уніфікованих методичних рекомендацій, які б можливо було застосувати для України, немає. Тож тематика дослідження є сучасною та актуальною.

Метою статті є проведення дослідження практичних підходів до боротьби з інформаційним тероризмом у системі міжнародного законодавства та міжнародних і національних інституцій провідних країн світу, а також аналіз норм міжнародного права у сфері протидії інформаційному тероризму з метою його практичного застосування в Україні. Підтвердження ефективності взаємодії державних органів і громадських організацій, об'єднань та окремих громадян у системі публічного управління у сфері протидії інформаційному тероризму.

Виклад основного матеріалу. Все світове співтовариство сьогодні стурбоване проблемами тероризму, а особливо його різновидом, як віхи світу, що постійно глобалізується, – інформаційного тероризму, оскільки це явище все більше загрожує безпеці багатьох країн і їхніх громадян. Мимоволі на думку приходять слова колишнього Генерального секретаря Організації Об'єднаних Націй Пана Гі Муна: «Інтернет є наочним прикладом того, як терористи можуть діяти дійсно на транснаціональної основі; у відповідь державам необхідно думати і діяти на настільки ж транснаціональної основі». І досвід Організації Об'єднаних Націй е цьому напрямі може бути безцінним.

За період із 1945 року міжнародне співтовариство напрацювало понад 50 міжнародних угод, спрямованих на запобігання терористичним проявам. Їх розроблення велося під егідою Організації Об'єднаних Націй (ООН) і Міжнародного агентства з атомної енергії (МАГАТЕ).

Серед зазначених документів особливо хотілося б виділити Глобальну контртерористичну стратегію ООН, прийняту у 2006 році. Відповідно до неї держави-члени співпрацюють із метою боротьби з тероризмом у всіх його формах і проявах у мережі Інтернет; а також для використання мережі Інтернет як інструмента боротьби з поширенням тероризму, визнаючи при цьому, що державам може знадобитися допомога в цих питаннях [4]. Стратегія містить 4 основні розділи:

– заходи щодо усунення умов, що сприяють поширенню тероризму;

– заходи щодо запобігання тероризму і боротьбі з ним;

– заходи зі зміцнення потенціалу держав щодо запобігання тероризму і боротьбі з ним і зміцненню ролі системи ООН у цій сфері;

– заходи щодо забезпечення загальної поваги прав людини і верховенства права як фундаментальної основи для боротьби з тероризмом.

На міжнародному і регіональному рівнях це вказує на постійно зростаючу небезпеку, що виходить від інформаційного тероризму.

Україна, як держава-член ООН, ратифікувала зазначені документи і здійснює взаємодію з питань боротьби з тероризмом, зокрема інформаційним, з міжнародними контртерористичними інституціями, що, у свою чергу, дає змогу враховувати досвід організаційного та законодавчого забезпечення й функціонування зарубіжних систем протидії інформаційному тероризму.

Та зауважимо, що всеосяжного документа ООН з питань боротьби з інформаційним тероризмом, який був би спеціально спрямований на запобігання і припинення використання телекомунікаційних технологій терористами, поки немає. До того ж міжнародне співтовариство досі не дійшло згоди щодо утвердження на міжнародному рівні єдиного визначення терміна «тероризм».

Огляд терористичних актів останніх років, скоєних у Швеції, Бельгії, Франції, Німеччині, Великобританії та Іспанії з використанням засобів підриву, автомобілів і підручних засобів, змусило владу європейських країн переглянути методи боротьби з тероризмом.

Наприклад, Великобританія, приділяючи значну увагу національному контртерористичному законодавству, у 2006 році прийняла Закон про тероризм, в частину 1 якого включено положення, що стосуються діяльності на базі інтернет-технологій та інших інформаційних технологій, які можуть підбурювати до вчинення терористичних актів або сприяти їх здійсненню. А навесні 2018 року влада Великої Британії ще більше посилила контртерористичні заходи, ввівши в дію новий закон про боротьбу з тероризмом і безпеки кордонів [5]. Також, згідно з положеннями нового акта, тепер протизаконно висловлювати будь-яку підтримку забороненим організаціям, а також публікувати зображення їхніх прапорів, емблем або форми, що дало б змогу припустити, що автор цих заяв і публікацій може або належати до заборонених організаціях, або бути їхнім прихильником.

З метою протидії поширенню екстремізму та тероризму в країні функціонують спеціальні органи, комітети, серед яких – управління міської поліції з боротьби з тероризмом, група безпеки електронних комунікацій при центрі урядового зв'язку.

Канцлер Німеччини Ангела Меркель підписала низку законів у сфері безпеки, що передбачали посилення відеоспостереження в громадських місцях, забезпечення поліцейських нагрудними камерами і використання автоматичних пристроїв для зчитування реєстраційних знаків транспортних засобів. А Федеральне відомство кримінальної поліції представило нову систему для оцінки ризику RADAR-iTE, розроблену спільно із судовими психологами з Константського університету [6]. Робота системи базується на аналізі відповідей на 73 стандартизованих запитання про соціалізацію людини, її ставлення до насильства, а також про її родинні зв'язки. На основі аналізу людині присвоюється одна з трьох категорій ризику: помірний, значний або високий.

Також уряд Німеччини схвалив Закон, що регулює використання даних пасажирів із систем бронювання авіакомпаній, які зобов'язані надавати країнам Євросоюзу дані про своїх пасажирів, щоб допомогти владі боротися з тероризмом та іншими серйозними злочинами.

Ще введено в дію Закон про комп'ютерне і мережеве спостереження. Він уповноважує владу країни зламувати комп'ютери, прослуховувати смартфони, а також отримувати доступ до листувань користувачів у месенджерах. Поліцейським Закон дозволяє використовувати шпигунське програмне забезпечення FinSpy, за допомогою якого можливо обійти шифрування і перехоплювати повідомлення в таких популярних месенджерах, як Whats App, Telegram і Signal.

Зараз майже всі Європейські країни, яких торкнулася хвиля терактів, працюють над модернізацією свого антитерористичного законодавства, включно з нормами, що регулюють механізми збору даних (відеоспостереження, прослуховування, реєстрація і передача даних про неповнолітніх і т. д.). До речі, в багатьох випадках законопроєкти були далеко не новими і протягом тривалого часу вони безуспішно лобіювались національними органами безпеки, натикаючись на великий опір у парламенті, і були прийняті тільки після терактів.

Але найефективнішим у довгостроковій перспективі заходом протидії тероризму в Європі експерти вважають боротьбу з пропагандою радикального ісламу. Мається на увазі блокування акаунтів, що поширюють пропаганду тероризму в соцмережах, введення кримінальної відповідальності за пропаганду тероризму в Інтернеті, посилення контролю за діяльністю мечетей (насамперед салафітських) і спроби виведення їх із-під контролю Саудівської Аравії, а також посилення інтернет-контролю за діяльністю ісламських організацій.

Не менш вагомими є надбання Сполучених Штатів Америки. 17 травня 2011 року президент Сполучених Штатів Америки Барак Обама підписав документ під назвою «Міжнародна стратегія розвитку кіберпростору» [7]. В опублікованій Стратегії вбачається суттєвий перегляд офіційної позиції США з питань інформаційної безпеки. Документ являє собою результат 20-річної історії формування системи державного забезпечення інформаційної безпеки в США.

Також великий інтерес становить військова стратегія кіберкомандування, створеного в червні 2009 року з метою протидії інформаційним загрозам національній безпеці США. До функцій кіберкомандування належать підготовка, координація, інтеграція, синхронізація дій із проведення операцій та захисту інформаційних мереж МО США і, в разі відповідного наказу, проведення військових інформаційних операцій по всьому спектру з метою забезпечення дій збройних сил у всіх сферах, забезпечення свободи дій американських і союзницьких збройних силу кіберпросторі, ураження інформаційних засобів противника.

Загалом, кількість організацій і відомств у США, задіяних у протидії інформаційному тероризму, досить велика. Серед них – Командування бойових дій у кібернетичному просторі (USCYBERCOM), Національний контртерористичний центр, Центр стратегічної контртерористичної взаємодії, до завдань якого входить координація співпраці із зарубіжними країнами з боротьби з тероризмом і екстремізмом. Усе це дає змогу США ефективніше, порівняно з іншими країнами, контролювати інтернет-простір. У 2015 році Америка заявила про початок нової фази в боротьбі проти екстремізму і тероризму в мережі, зосередивши основну увагу правоохоронних і спеціальних служб на Інтернеті, що став дуже зручним засобом для радикальних ідеологів із вербування нових членів у злочинні мережі.

Характерним для Ізраїлю є не стільки вплив органів державної влади на забезпечення антитерористичної безпеки, скільки активна участь громадських недержавних організацій у популяризації недопущення будь-яких проявів тероризму. Зокрема, активну роль забезпечення антитерористичної безпеки в Ізраїлі відіграє Інститут міжнародної політики з боротьби з тероризмом – некомерційна організація, яка ставить на меті боротьбу з тероризмом у всьому світі, оцінку ризиків і загроз, аналітичну розвідку, забезпечення національної безпеки [8]. Характерною особливістю діяльності громадських недержавних організацій Ізраїлю є активна робота з населенням щодо поширення інформації. Так вибудовується загальна суспільна думка, що не тільки держава, а й кожен громадянин самостійно повинен піклуватися про свою особисту безпеку. Така форма взаємодії громадських організацій у взаємодії з профільними спецслужбами, на нашу думку, сьогодні дуже актуальна для України на шляху побудови публічної політики протидії інформаційному тероризму, особливо протидії йому щодо проявів навколо конфлікту на сході країни.

Велике значення у сфері запобігання тероризму також має Ізраїльська антитерористична стратегія. Тобто в Ізраїлі законодавець, а також правоохоронні органи в питаннях боротьби з інформаційним тероризмом головну ставку роблять на недержавні організації боротьби з цим злочинним явищем як вагомим провідником і зв'язуючою ланкою між державою та громадянами.

Проте на міжнародному рівні, за відсутності будь-яких універсальних документів, що накладають пряме зобов'язання прийняти законодавство, спеціально спрямоване проти інформаційного тероризму, більша частина урядів вважає за краще боротися з такими загрозами, дотримуючись змішаного підходу, використовуючи комбінацію загального кримінального законодавства та законодавства про боротьбу з кіберзлочинністю і тероризмом. У низці держав, наприклад, головна увага в кримінальному законодавстві приділяється основним злочинам без їх диференціації за конкретними засобами, за допомогою яких вони здійснюються. Відповідно до цього підходу інформаційний простір розглядається лише як засіб, за допомогою якого терористи здійснюють злочини, нерідко позначені в положеннях національного кримінального кодексу. Цей підхід характерний для Китаю, Японії, Республіки Корея.

Водночас важливу роль у забезпеченні контролю за доступом до поширюваного засобами комунікацій контенту, пов'язаного з терористичною діяльністю, продовжує відігравати приватний сектор (ЗМІ, медіа, провайдери послуг, вебсайти, що надають послуги з розміщення користувацького контенту, інтернет-пошуковики). Стимулом до співпраці їх із правоохоронними органами може стати позитивний вплив такого співробітництва на їхню репутацію в питаннях дотримання прав людини, свободи вираження думок, поваги недоторканності приватного життя, житла і кореспонденції, а також права на захист інформації. На рівень співпраці також може впливати страх відповідальності у зв'язку з розміщенням певних видів інтернет-контенту.

Наприклад, у 2010 році після консультацій з урядами Сполученого Королівства і Сполучених Штатів корпорація Google Inc., що є компанією-засновником YouTube, добровільно ввела систему, яка дала можливість користувачам контенту позначати потенційно пов'язаний із тероризмом контент на вебсайті YouTube. Цей механізм є важливим засобом попереджувального виявлення контенту, який може сприяти вчиненню терористичних актів.

Служба розшуку міжнародних терористичних організацій (SITE) і мережа «Інтернет-Хагана» в США ведуть моніторинг терористичних організацій із відкритих джерел. Служба і подібні до неї організації оперативно виявляють матеріали про терористичну діяльність в Інтернеті. «Інтернет-Хагана», навпаки, відстежує діяльність ісламістських екстремістських груп в Інтернеті з метою виявлення контенту, пов'язаного з тероризмом, і припинення доступу до нього. Ця служба ділиться відповідною інформацією з правоохоронними органами з метою сприяння боротьбі з інформаційним тероризмом. Хоча цілі і способи функціонування цих служб моніторингу відрізняються, обидві вони своїми діями сприяють швидкому виявленню інформаційного тероризму.

На думку фахівців, створення спрямованих на протидію інформаційному тероризму партнерств між зацікавленими сторонами в державному і приватному секторах може принести чимало потенційних переваг. Серед проблем на шляху розвитку співпраці між державним і приватним сектором у сфері боротьби з інформаційним тероризмом аналітики нерідко визначають недостатність належних контактів між правоохоронними органами та провайдерами інформаційних послуг із питань забезпечення ефективного збору доказів у царині протиріч між принципом недоторканності приватного життя і необхідністю збереження даних у правозастосовних цілях. Створення форуму для ведення офіційного і неофіційного діалогу між партнерами з державного та приватного секторів могло б істотно знизити гостроту таких проблем.

Прикладом успішного державно-приватного партнерства, пов'язаного із забезпеченням інформаційної безпеки, може також бути Консультативна рада з питань безпеки за кордоном, створена спільно Державним департаментом Сполучених Штатів і американськими організаціями приватного сектору. Рада служить форумом для обміну передовим досвідом, а також платформою для регулярного і своєчасного обміну інформацією між приватним сектором і урядом Сполучених Штатів щодо подій у сфері безпеки за кордоном, зокрема, у зв'язку з діяльністю терористів, а також політичних, економічних і соціальних факторів, які можуть впливати на стан безпеки в глобальному масштабі і за окремими країнами.

Індонезійська Група реагування на інциденти, пов'язані з інформаційною безпекою (MASTEL), є ще одним прикладом ініціативи зі створення партнерства між державним і приватним сектором. Вона об'єднує представників служб пошти та електрозв'язку, національної поліції, Генеральної прокуратури, Банку Індонезії, Індонезійської асоціації провайдерів інтернет-послуг, Індонезійської асоціації інтернет-кафе, Індонезійської асоціації емітентів кредитних карт. Її члени співпрацюють, зокрема, з метою проведення моніторингу, виявлення проблем і збоїв у телекомунікаційних мережах і раннього оповіщення про них; здійснення досліджень і розробок; організації лабораторного моделювання і професійної підготовки з питань безпечного використання телекомунікаційних мереж; надання консультативних послуг і технічної допомоги стратегічно важливим відомствам або установам; а також виконання функцій координаційного центру для відповідних відомств або установ – як внутрішніх, так і міжнародних.

Отже, незважаючи на зростаюче за останні роки міжнародне визнання інформаційного тероризму, сьогодні необхідні правоохоронним органам повноваження багато в чому схожі, незалежно від конкретної юрисдикції, про яку йдеться, а відмінності в національній політиці і законодавстві є відображенням різноманіття правових систем, конституційних положень та інших факторів (наприклад, культури).

Тому на міжнародному рівні є потреба у створенні та впровадженні уніфікованого нормативно-правового забезпечення (так званого типового законодавства), яке, не створюючи юридичних зобов'язань, мало б характер рекомендаційних керівних принципів, відігравало б важливу роль у процесі приведення у відповідність прийнятих державами правових стандартів. На відміну від міжнародних конвенцій, укладення яких може бути пов'язане з проведенням ґрунтовних переговорів із метою врахування потреб широкого кола потенційних підписантів, положення типових законів дали б державам можливість скористатися зводом ефективних базових правових норм як відправної точки для розроблення внутрішнього законодавства.

Наприклад, з метою припинення процесу радикалізації та насадження екстремістських ідеалів урядами країн можуть використовуватися такі ефективні засоби, як контрпропаганда і поширення різних повідомлень стратегічного характеру.

Висновки з дослідження і перспективи подальших розвідок у цьому напрямі. Підбиваючи підсумки огляду міжнародного законодавства та міжнародних і національних інституцій у сфері боротьби з інформаційним тероризмом, хотілося б окреслити декілька висновків, осмислення яких, на наше переконання, допомогло б використати їх для вдосконалення вітчизняного механізму протидії інформаційному тероризму:

1. Потребує вдосконалення антитерористичне нормативно-правове забезпечення з метою впровадження кримінальної відповідальності за вчинення інформаційних терористичних актів, а також напрацювання на законодавчому рівні єдиного понятійного апарату в цій сфері.

2. Необхідно вдосконалити управлінську ланку координації протидії інформаційному тероризму з метою підвищення рівня оперативності реагування і прийняття рішень на найвищому державному рівні на ці злочинні прояви.

3. Потребує розширення і спрощення слідчих повноважень правоохоронних органів, що займаються справами, пов'язаними зі злочинами терористичного характеру, зокрема інформаційним тероризмом.

4. Серед населення необхідно запровадити практику публічного роз'яснення основних заходів державної протидії інформаційному тероризму (обов'язково із зазначенням позитивних результатів, що має заспокоїти людей), залучення на добровільній основі до деяких заходів соціальних неурядових організацій.

5. Необхідно напрацювати спеціальні процедури судочинства і надання доказів у сфері прийняття вироків суду по судовим справам інформаційного тероризму.

І найголовніше те, що в Україні, так само як і в Європейських та інших країнах, державна система боротьби з інформаційним тероризмом дуже розрізнена (іноді змішана): сьогодні суб'єкти, що безпосередньо здійснюють

боротьбу з тероризмом, та ті, що можуть залучатися до заходів боротьби з тероризмом, виконують завдання боротьби з інформаційним тероризмом по-різному (по-своєму, з урахуванням відомчих характерів провадження своєї професійної діяльності). Тому сьогодні необхідно уніфікувати законодавство у сфері боротьби з інформаційним тероризмом, спираючись на міжнародний досвід, а також запровадити єдину державну систему протидії цьому злочинному явищу. Усе це можливо здійснити лише за умови чіткого уповноваження на це державного органу, наділеного вітчизняним законодавством функціями координації антитерористичної діяльності – Антитерористичного центру при Службі безпеки України.

Список використаних джерел:

1. Ліпкан В., Максименко Ю., Желіховський В. Інформаційна безпека України в умовах євроінтеграції. 2006. С. 15. URL: http://www.dut.edu.ua/ua/lib/1/category/1181/view/1350.
2. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами. *Альманах економічної безпеки*. 1999. № 2. С. 15–17.
3. Радковець Ю., Левченко О., Косогов О. Погляди на створення системи інформаційної безпеки України та її Збройних Сил. *Наука і оборона*. 2014. № 1. С. 38–42.
4. Глобальна контртерористична стратегія ООН. URL: https://www.un.org/counterterrorism/ctitf/ru/un-global-counter-terrorism-strategy.
5. Закон про боротьбу з тероризмом Великобританії. URL: https://www.gov.uk/government/collections/counter-terrorism-and-border-security-bill-2018#history.
6. Інструмент оцінки ризиків RADAR-iTE. URL: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2017/Presse2017/170202_Radar.html.
7. International Strategy for Cyberspace. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cybersecurity-strategies-ncsss/international_strategy_for_cyberspace_US.pdf.
8. Інститут міжнародної політики по боротьбі з тероризмом. URL: http://www.ictaconline.com/?page_id=12.

References:

1. Lipkan V., Maksimenko U. and Zhelikhovsky V. (2006), Informacijna bezpeka Ukrajiny v umovakh jevrointeghraciji [Information Security of Ukraine in the Minds of Integration]. 15 p. URL: http://www.dut.edu.ua/ua/lib/1/category/1181/view/1350.
2. A. Katrenko (1999), Osoblivosti informatsiynoi baezpeki za mizhnarodnimi standartami [Features of information security by international standards] journal *Almanah economichnoi bezpeki* [Almanac of economic security]. Vol. 2, pp. 15–17 [Ukraine].
3. Radkovets U., Levchenko O. and Kosogov O. (2014), Poglyady na stvorennya sistemi informatsiynoi bezpeki Ukrainy ta ii Zbroynih Syl [Views on the creation of the information security system of Ukraine and its Armed Forces] journal *Nauka i oborona* [Science and Defense]. Vol. 1, pp. 38–42 [Ukraine].
4. UN Global Counter-Terrorism Strategy. URL: https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy.
5. UK Anti-Terrorism Law. URL: https://www.gov.uk/government/collections/counter-terrorism-and-border-security-bill-2018#history.
6. RADAR-iTE Risk Assessment Tool. URL: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2017/Presse2017/170202_Radar.html.
7. International Cyberspace Strategy. URL: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cybersecurity-strategies-ncsss/international_strategy_for_cyberspace_US.pdf.
8. Institute for International Policy on Combating Terrorism. URL: http://www.ictaconline.com/?page_id=12.