УДК 343.341:323.28(477)

ТКАЧОВ Іван Валентинович

ІНФОРМАЦІЙНА СКЛАДОВА ТЕРОРИСТИЧНОЇ ЗАГРОЗИ: ПРАВОВЕ ЗАКРІПЛЕННЯ В УКРАЇНІ

Постановка проблеми. На сьогодні інформаційна складова терористичної загрози стала одним із найважливіших елементів забезпечення антитерористичної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура й інформаційні технології не лише впливають на рівень і темпи розвитку суспільства та держави, а й стають засобами гібридної, інформаційної війни [1, с. 82].

Аналіз останніх досліджень і публікацій. У розробку проблематики виявлення та нейтралізації терористичних загроз, їхніх складових, забезпечення антитерористичної безпеки суттєвий внесок зробили такі дослідники: В. Ф. Антипенко, О. П. Богданов, Н. М. Варенья, В. О. Глушков, В. П. Ємельянов, О. А. Івахненко, В. В. Крутов, С. С. Кудінов, Б. Д. Леонов, В. А. Ліпкан, В. В. Остроухов, Л. М. Стрельбицька, М. П. Стрельбицький, В. І. Строгий та інші [1–4]. Водночас питання використання правового закріплення терористичної загрози, використання інформаційного простору, ресурсів, інфраструктури та технологій детально не розглядалися.

Метою статті є аналіз концептуальних положень вітчизняного законодавства на предмет правового закріплення терористичної загрози, насамперед її інформаційної складової.

Виклад основного матеріалу. У Концепції боротьби з тероризмом 2019 року антитерористична безпека держави визначається як захищеність об'єктів можливих терористичних посягань від терористичних загроз. До об'єктів можливих терористичних посягань разом з іншим належать інформаційний простір та його компоненти, стосовно яких можуть вчинятися терористичні акти. Під терористичною загрозою розуміються існуючі та потенційно можливі чинники, що створюють небезпеку вчинення терористичного акту щодо об'єкта можливих терористичних посягань та настання негативних наслідків від нього [5].

Разом із терміном «терористична загроза» в наукових джерелах використовуються також «загроза терористичного характеру», «терористичне посягання», «терористичний прояв» та інші, які не визначені в нормативно-правових актах України. Не вдаючись до полеміки щодо цих

понять, розглянемо докладніше інформаційну складову терористичної загрози.

В аналітичній доповіді Національного інституту стратегічних досліджень виокремлені актуальні тенденції в розвитку міжнародного тероризму, зокрема: прагнення до використання терористичними організаціями нових технологій і розширення активності в кіберпросторі: розповсюдження пропаганди; проведення вербувальної роботи; підтримання зв'язку зі своїми осередками (зокрема через закриті інформаційні мережі типу Даркнет та з використанням новітніх методів шифрування); надання своїм прихильникам і послідовникам інструкцій щодо особливостей підготовки та здійснення терористичних атак; протиправна діяльність у кіберпросторі, пов'язана із здійсненням хакерських атак; викрадення даних тощо. Сьогодні у вільному доступі супутникові знімки будь-якої місцевості або потенційного об'єкта терористичної атаки, а системи онлайн-платежів суттєво спрощують проведення фінансових операцій, пов'язаних із забезпеченням злочинної діяльності. За різними оцінками, існує не менше 5 000 сайтів, створених терористичними організаціями [6, с. 7].

У підсумку фахівці НІСД дійшли висновку, що з розвитком технологій розширюватиметься діяльність терористичних організацій у кіберпросторі, розвиватимуться методи інформаційно-пропагандистської роботи. Загрозливою тенденцією є активне залучення до терористичної діяльності безпосередньо громадян країн, які є об'єктами терористичних нападів [6, с. 46].

Тому важливе своєчасне проведення аналізу нормативно-правових актів України загальнодержавного рівня на предмет закріплення в них терористичних загроз безпеці держави й насамперед інформаційної складової.

Чинна Стратегія національної безпеки України «Безпека людини – безпека країни», затверджена Указом Президента України 14 вересня 2020 року [7], до поточних та прогнозованих загроз національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов (розділ 2) відносить, зокрема:

– поширення міжнародного тероризму (пункт 10);

– укорінення радикальних суспільних настроїв і середовищ, які є основою для поширення тероризму (пункт 23).

У розділі 3 «Основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки» Стратегії визначається, що Україна, прагнучи зміцнити заснований на демократичних нормах і цінностях міжнародний порядок, бере активну участь у протидії тероризму (пункт 33).

До пріоритетних завдань правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їхньої компетенції зокрема віднесено:

– активну та ефективну протидію спеціальним інформаційним операціям і кібератакам, російській та іншій підривній пропаганді;

– запобігання, виявлення та припинення проявів сепаратизму, тероризму, екстремізму, припинення діяльності незаконних збройних формувань, політично мотивованого насильства та інших зазіхань на конституційний лад (пункт 45) [7].

Отже, Стратегія національної безпеки України не пов'язує терористичну загрозу із загрозами в інформаційній сфері, інформаційній безпеці держави.

По-іншому до цього питання підійшли розробники Концепції розвитку сектору безпеки і оборони України 2016 року [8]. Так, серед кризових ситуацій визначено провадження на території України суспільно небезпечної діяльності в кіберпросторі (або з використанням його технічних можливостей) із терористичною метою шляхом застосування сучасних інформаційно-комунікаційних технологій (підпункт 4 пункту 10).

Надаючи оцінку безпековому середовищу нашої держави, Концепція до найактуальніших загроз відносить, зокрема, дії, спрямовані на розпалювання міжетнічної, міжконфесійної, соціальної ворожнечі та ненависті, сепаратизму й тероризму. Основною формою гібридної війни проти України є комбінація різноманітних і динамічних дій регулярних сил Російської Федерації, що взаємодіють зі злочинними озброєними угрупованнями й кримінальними елементами, діяльність яких координується та здійснюється за єдиним замислом і планом з активним застосуванням засобів пропаганди, саботажу, навмисного завдання шкоди, диверсій і терору.

При проведенні оцінювання стану складових сектору безпеки і оборони з'ясовано, що невирішеною проблемою є недостатня ефективність діяльності суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам терористичного характеру [8].

У чинній Стратегії кібербезпеки України 2016 року [9] при визначенні загроз кібербезпеці констатується, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури. Активно поширюється політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі «Інтернет».

При визначенні національної системи кібербезпеки та основних суб'єктів забезпечення кібербезпеки Стратегія покладає на Службу безпеки України такі основні завдання: здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом і кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів.

У цьому контексті слід зазначити, що робоча група при Національному координаційному центрі

кібербезпеки Ради національної безпеки і оборони України схвалила проєкт Стратегії кібербезпеки України на 2021–2025 роки [10]. У ньому в розділі про глобальний контекст кібербезпеки зазначено, зокрема, що масштабу глобального тренда набуває використання кіберпростору терористичними організаціями (кібертероризм). Цьому сприятиме всеосяжна цифрова трансформація систем управління та життєзабезпечення, що невпинно розширює цільову аудиторію кібертероризму та спектр потенційних об'єктів кібератак. Пріоритетними об'єктами терористичних кібератак вважаються об'єкти атомної енергетики, системи управління електропостачанням, авіа- та залізничним транспортом, потужні сховища стратегічних видів сировини, системи водопостачання, хімічні й біологічні об'єкти [10]. У контексті загроз зазначено, що в Україні останніми роками відчутно зросла загроза кібертероризму. Насамперед це пов'язано з кіберможливостями держави-агресора Російської Федерації, яка веде проти України кібервійну із застосуванням кіберзброї. Спостерігається використання кіберпростору для фінансування терористичних угруповань [10].

Отже, проєкт Стратегії кібербезпеки України передбачає більший за обсягом спектр терористичної загрози, що вказує на те, що його розробники врахували сучасний стан суспільно-політичної ситуації на сході держави, загальні тенденції та можливості тероризму в інформаційній сфері.

Концепція боротьби з тероризмом в Україні 2019 року [5] до об'єктів можливих терористичних посягань серед інших відносить інформаційний простір та його компоненти. З-поміж напрямів реалізації Концепції (розділ 3) визначено підвищення рівня поінформованості суспільства про небезпеку та масштаби тероризму.

Антитерористичне забезпечення об'єктів можливого терористичного посягання передбачає вирішення, разом з іншими, завдань з удосконалення законодавства у сфері інформаційної безпеки держави, зокрема в частині підвищення рівня захищеності населення від негативних інформаційно-психологічних впливів [5].

Із метою реалізації Концепції боротьби з тероризмом в Україні підготовлено відповідний План заходів з реалізації Концепції боротьби з тероризмом в Україні, який передбачає такі заходи:

– забезпечувати проведення аналізу стану й тенденцій поширення тероризму, причин і умов, що впливають на його виникнення та поширення, ефективності законодавства у сфері боротьби з тероризмом і за його результатами внесення в установленому порядку пропозицій щодо підвищення ефективності заходів боротьби з тероризмом, зокрема щодо підвищення рівня захищеності населення від негативних інформаційно-психологічних впливів;

– забезпечити обмін досвідом суб'єктів боротьби з тероризмом з відповідними органами іноземних держав та міжнародними організаціями з метою підвищення ефективності

боротьби з тероризмом в Україні, недопущення використання кіберпростору в терористичних цілях.

Висновки. Інформаційний простір України та його компоненти є об'єктом можливих терористичних посягань. Закріплення в нормативно-правових актах України загальнодержавного рівня інформаційної складової терористичної загрози вказує на такі можливі способи реалізації цієї загрози:

– суспільно небезпечна діяльність у кіберпросторі (або з використанням його технічних можливостей) із терористичною метою шляхом застосування сучасних інформаційно-комунікаційних технологій;

– діяльність збройних сил у взаємодії із злочинними угрупованнями із застосуванням засобів тероризму як один із проявів гібридної війни;

– використання сучасних інформаційно-комунікаційних технологій для здійснення терористичних актів шляхом посягань на роботу автоматизованих систем управління технологічними процесами на об'єктах критичної інфраструктури;

– вчинення актів кібертероризму стосовно інформаційної інфраструктури;

– використання кіберпростору терористичними організаціями;

– використання кіберпростору для фінансування терористичних угруповань.

У перспективі на загальнодержавному рівні виокремлюється категорія «пріоритетні об'єкти терористичних кібератак», до яких належать: об'єкти атомної енергетики, системи управління електропостачанням, транспортом, потужні сховища стратегічних видів сировини, системи водопостачання, хімічні й біологічні об'єкти.

Подальші наукові дослідження доцільно спрямувати на питання взаємозв'язку інформаційного простору та його компонентів як об'єктів можливих терористичних посягань з іншими складовими терористичної загрози: соціальною, економічною, технологічною тощо.

Рецензенти:
доктор юридичних наук, професор,
заслужений юрист України
І. Рижов,
кандидат юридичних наук
А. Коростиленко

Список використаних джерел

1. Рижов І. М., Стрельбицька Л. М., Стрельбицький М. П., Строгий В. І. Виклики тероризму в Україні та адекватні концепти державної безпеки : навчальний посібник. Київ : Нац. акад. СБУ, 2015. 172 с.

2. Рижов І. М. Базові концепти антитерористичної безпеки : монографія / Нац.

акад. Служби безпеки України. Київ : Нац. акад. СБУ, 2016. 327 с.

3. Кудінов С. С., Рижов І. М., Івахненко О. А. Основи антитерористичної безпеки соціальних систем : монографія. Київ : Кафедра, 2017. 212 с.

4. Рижов І. М. Парадигмальні риси антитерористичної безпеки сучасного інформаційного суспільства // Інформаційна безпека людини, суспільства, держави. 2019. № 3 (27). С. 110–118.

5. Концепція боротьби з тероризмом в Україні, затверджена Указом Президента України від 5 березня 2019 року № 53/2019. URL: http://zakon.rada.gov.ua (дата звернення: 09.09.2020).

6. Резнікова О. О., Місюра А. О., Дрьомов С. В., Войтовський К. Є. Актуальні питання протидії тероризму у світі та в Україні : аналітична доповідь / за заг. ред. О. О. Резнікової. Київ : НІСД, 2017. 60 с.

7. Стратегія національної безпеки України «Безпека людини – безпека країни», затверджена Указом Президента України від 14 вересня 2020 року № 392/2020. URL: http://zakon.rada.gov.ua (дата звернення: 19.09.2020).

8. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» : Указ Президента України від 14 березня 2016 року № 92/2016. URL: http://www.rnbo.gov.ua/documents/418.html (дата звернення: 09.09.2020).

9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016. URL: http://zakon.rada.gov.ua (дата звернення: 09.09.2020).

10. Робоча група при НКЦК РНБО України схвалила проєкт Стратегії кібербезпеки України. URL: https://www.rnbo.gov.ua (дата звернення: 09.09.2020).

Аннотация. Статья посвящена исследованию правового закрепления информационной составляющей террористической угрозы в нормативно-правовых актах Украины общегосударственного уровня.

Проанализированы: Стратегия национальной безопасности Украины 2020 года, Концепция развития сектора безопасности и обороны Украины 2016 года, Стратегия кибербезопасности Украины 2016 года, проект новой Стратегии кибербезопасности Украины на 2021–2025 годы, Концепция борьбы с терроризмом в Украине 2019 года, План мер по реализации Концепции борьбы с терроризмом в Украине.

Отмечается, что реализация террористической угрозы в информационной сфере проявляется в виде: общественно

Abstract. The article is devoted to the research of legal confirmation of information component of terrorist threat in legal acts of Ukraine at the nationwide level.

The article suggests analysis of 2020 National Security Strategy of Ukraine, 2016 Concept of Security and Defense Sector of Ukraine Development, 2016 Strategy of Cybersecurity of Ukraine, the draft of the new Strategy of Cybersecurity of Ukraine for the period of 2021–2025, 2019 Counter-Terrorism Concept of Ukraine and the Action Plan of Implementation of Counter-Terrorism Concept of Ukraine.

It is noted that the implementation of the terrorist threat in the information sphere is manifested in the form of: socially dangerous activities in cyberspace with a terrorist purpose; collaboration of armed forces with organized crime groups using terrorist means as one of the manifestations of hybrid

опасной деятельности в киберпространстве с террористической целью; деятельности вооруженных сил во взаимодействии с преступными группами с использованием средств терроризма как одно из проявлений гибридной войны; использования современных информационно-коммуникационных технологий для проведения террористических актов путем посягательств на работу автоматизированных систем управления технологическими процессами на объектах критической инфраструктуры; использования киберпространства террористическими организациями для финансирования терроризма; осуществления актов кибертерроризма в отношении информационной инфраструктуры.

На общегосударственном уровне выделяется такая категория как приоритетные объекты террористических кибератак (объекты атомной энергетики, системы управления электроснабжением, транспортом, большие хранилища стратегических видов сырья, системы водоснабжения, химические и биологические объекты).

Ключевые слова: антитеррористическая безопасность, террористическая угроза, информационное пространство, кибертерроризм, информационная инфраструктура.

war; using the modern information and communication technologies for conducting terrorist acts by the intrusion to the automated control systems of the technological processes in the critical infrastructure facilities; using modern information and communications technologies for carrying out terrorist acts by encroaching on the operation of automated control systems for technological processes at critical infrastructure facilities; using cyberspace by terrorist organizations to finance terrorism; carrying out acts of cyberterrorism against information infrastructure.

At the nationwide level, such category as priority targets for terrorist cyberattacks is distinguished (nuclear power facilities, power supply and transport management systems, large storage facilities for strategic raw materials, water supply systems, chemical and biological facilities).

Key words: anti-terrorist security, terrorist threat, information space, cyberterrorism, information infrastructure.