Національна безпека та державна охорона

Адміністративне право і процес; фінансове право; інформаційне право

УДК 342.056.53

Скриньковський Руслан Миколайович

кандидат економічних наук, професор

Львівський університет бізнесу та права

Skrynkovskyy Ruslan

PhD in Economics, Professor

Lviv University of Business and Law

ORCID: 0000-0002-2180-8055

Ковалів Мирослав Володимирович

кандидат юридичних наук, професор

Львівський державний університет внутрішніх справ

Kovaliv Myroslav

PhD in Law, Professor

Lviv State University of Internal Affairs

ORCID: 0000-0002-9730-8401

Єсімов Сергій Сергійович

кандидат юридичних наук, професор

Львівський державний університет внутрішніх справ

Yesimov Serhii

PhD in Law, Professor

Lviv State University of Internal Affairs

ORCID: 0000-0002-9327-0071

Перепелиця Анатолій Васильович
кандидат юридичних наук, доцент
Львівський державний університет внутрішніх справ
Perepelytsia Anatoliy
PhD in Law, Associate Professor
Lviv State University of Internal Affairs
ORCID: 0000-0002-8378-0879

ПРАВОВЕ РЕГУЛЮВАННЯ ПРОТИДІЇ ВИКОРИСТАННЮ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У ТЕРОРИСТИЧНИХ ЦІЛЯХ

LEGAL REGULATION OF COUNTERING THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES FOR TERRORIST PURPOSES

Анотація. *Вступ. Забезпечення протидії використанню терористами нових технологічних рішень має всеосяжний характер. Запобігання цій загрозі потребує поєднання не лише силових та оперативних заходів реагування держави, а й повномасштабної реформи правового регулювання відповідних суспільних відносин. Зазначені обставини стали основою вибору теми дослідження.*

Мета. Метою статті є дослідження правового регулювання протидії використанню інформаційно-комунікаційних технологій у терористичних цілях.

Матеріали і методи. Матеріалами дослідження є література, яка стосується правового регулювання протидії використанню інформаційно-комунікаційних технологій. Методологічну основу дослідження складають

комплексний системний аналіз правових явищ, загальнонаукові методи пізнання, включаючи аналіз, синтез, опис, узагальнення, аналогію, та приватно-правові методи: формально-юридичний, порівняльно-правовий.

Результати. Обґрунтовано, що в умовах нового цифрового середовища технологічні досягнення в інформаційній сфері, включаючи технології штучного інтелекту та робототехніку, можуть використовуватися з метою організації, підготовки або вчинення терористичних актів, для здійснення комп'ютерних атак на об'єкти інформаційної інфраструктури, включаючи критичну. У зв'язку з цим виявлено тенденцію до формування міжгалузевого комплексного інституту протидії використанню інформаційно-комунікаційних технологій у терористичних цілях. До структури цього інституту, поряд із інформаційно-правовими нормами, входять норми різних галузей права (у тому числі адміністративного та кримінального), які об'єднані базовим поняттям в інформаційній сфері – «інформація». Також актуальним і важливим питанням, враховуючи сучасні загрози та виклики, є удосконалення взаємодії Служби безпеки України та Управління державної охорони України у забезпеченні національної безпеки України.

Перспективи. Подальші наукові дослідження повинні охоплювати необхідність удосконалення та розвитку національної системи документів стратегічного планування у сфері забезпечення інформаційної безпеки та протидії тероризму відповідно до стандартів Європейського Союзу та НАТО.

Ключові слова: *правове регулювання, протидія тероризму, терористичний акт, інформаційно-комунікаційні технології, інформаційна безпека, суб'єкти боротьби з тероризмом, Служба безпеки України, Управління державної охорони України, норми права, законодавство України,*

НАТО.

Summary. *Introduction. Ensuring countermeasures against the use of new technological solutions by terrorists is comprehensive in nature. Prevention of this threat requires a combination of not only forceful and operational response measures of the state, but also a full-scale reform of the legal regulation of relevant social relations. The specified circumstances became the basis for choosing the research topic.*

Purpose. The purpose of the article is to research the legal regulation of combating the use of information and communication technologies for terrorist purposes.

Materials and methods. The materials of the study are the literature related to the legal regulation of opposition to the use of information and communication technologies. The methodological basis of the research consists of a complex systematic analysis of legal phenomena, general scientific methods of cognition, including analysis, synthesis, description, generalization, analogy, and private legal methods: formal-legal, comparative-legal.

Results. It is substantiated that in the conditions of the new digital environment, technological achievements in the information field, including artificial intelligence technologies and robotics, can be used to organize, prepare or commit terrorist acts, to carry out computer attacks on information infrastructure objects, including critical ones. In this regard, a trend towards the formation of an interdisciplinary complex institute for combating the use of information and communication technologies for terrorist purposes was revealed. The structure of this institute, along with information and legal norms, includes norms of various branches of law (including administrative and criminal), which are united by the basic concept in the information sphere – «information». Also, a

relevant and important issue, taking into account modern threats and challenges, is the improvement of cooperation between the Security Service of Ukraine and the Department of the State Protection of Ukraine in ensuring the national security of Ukraine.

Prospects. Further scientific research should cover the need to improve and develop the national system of strategic planning documents in the field of ensuring information security and combating terrorism in accordance with the standards of the European Union and NATO.

Key words: *legal regulation, counter-terrorism, terrorist act, information and communication technologies, information security, entities fighting terrorism, Security Service of Ukraine, Department of the State Protection of Ukraine, legal norms, legislation of Ukraine, NATO.*

Постановка проблеми. XXI століття внесло в життя людини безліч можливостей для реалізації свого потенціалу та покращення якості життя. Це стало можливим завдяки розвитку інформаційно-комунікаційної сфери, забезпеченню швидкісного доступу до мережі Інтернет і впровадженню технологій штучного інтелекту практично в усі сфери суспільного життя. Водночас цифровізація та посилення технологічної залежності суспільства і держави характеризуються можливістю застосування технологічних досягнень у протиправних цілях і використанням інформаційного простору в терористичній діяльності. Це особливо актуально сьогодні, оскільки агресія росії проти України сприяє збільшенню загрози поширення пропаганди тероризму та здійснення комп'ютерних атак на критичну інформаційну інфраструктуру для досягнення російських терористичних цілей.

Аналіз останніх досліджень і публікацій (стан опрацювання проблематики). Забезпечення інформаційної безпеки у контексті протидії

використанню інформаційно-комунікаційних технологій у терористичних цілях досліджували вчені: С. Білько, С. Гнатюк, М. Григорчук, О. Дзьобань, О. Довгань, О. Золотар, О. Косілова, С. Кудін, В. Ліпкан, О. Логінов, М. Микитюк, Н. Новицька, Т. Ткачук, О. Тихомиров, В. Цимбалюк, А. Шевченко, О. Ярема та інші. Розвиток технічних засобів у сфері інформаційних технологій вимагає проведення наукових досліджень у всіх галузях юридичної науки, у тому числі щодо правового регулювання протидії використанню інформаційно-комунікаційних технологій у терористичних цілях.

Мета статті. Метою статті є дослідження правового регулювання протидії використанню інформаційно-комунікаційних технологій у терористичних цілях.

Виклад основного матеріалу дослідження. У XXI столітті розвиток інформаційно-комунікаційних технологій (далі – ІКТ) відіграє ключову роль у цифровій трансформації суспільства та держави. Потенціал ІКТ сьогодні реалізується в різних сферах – починаючи від повсякденного життя громадян і закінчуючи державним управлінням у сфері національної безпеки. Посилення технологічної залежності суспільства і держави водночас характеризується необхідністю розробки належного правового забезпечення протидії новим викликам і загрозам, які породжуються прискореним розвитком інформаційного середовища поряд із політичними процесами, що відбуваються сьогодні, та прискорюють адаптацію нормативних актів у вказаній сфері Європейського Союзу та НАТО, у тому числі з питань забезпечення інформаційної безпеки, появою нових можливостей використання технологічних досягнень у протиправних цілях, включаючи терористичні.

У Стратегії національної безпеки України «Безпека людини – безпека

країни», затвердженої Указом Президента України від 14.09.2020 р. № 392/2020, та Стратегії інформаційної безпеки України, затвердженої Указом Президента України від 28.12.2021 р. № 685/2021, серед завдань, спрямованих на досягнення мети щодо забезпечення інформаційної безпеки України, виділяється, зокрема, протидія використанню інформаційної інфраструктури України терористичними організаціями. Це, у свою чергу, ставить перед законодавцем завдання щодо розвитку правового регулювання суспільних відносин, пов'язаних із формуванням ефективної системи протидії використанню ІКТ у терористичних цілях [1; 2].

Все це зумовлює необхідність дослідження теоретичних положень, включаючи питання визначення місця в системі права, і зокрема, інформаційного права, сукупності правових норм, спрямованих на регулювання протидії використанню ІКТ у терористичних цілях, які містяться у різних нормативно-правових актах – багатосторонніх та двосторонніх міжнародних угодах України про співробітництво у сфері забезпечення інформаційної безпеки, у законах і кодифікованих актах.

З метою дослідження питання про місце в інформаційному праві зазначених норм слід відзначити загальну тенденцію стрімкої трансформації системи права України, в якій інформаційно-правова сфера не є винятком і повною мірою відображає кардинальні зміни, що відбуваються.

У зв'язку з цим необхідно звернути увагу на твердження М. Бліхар [3], яка виділяє серед основних завдань в умовах цифрової трансформації побудову галузевої та інституційної структури правової системи інформаційного права. Також М. Бліхар та Ю. Мельник відзначають посилення процесу інституалізації інформаційного права, що має міждисциплінарний характер [3, с. 308].

З'ясовано, що комплекс правових норм, які регулюють суспільні

відносини щодо протидії використанню ІКТ у терористичних цілях, слід відносити до такого роду нових міжгалузевих правових інститутів, що формуються. Для обґрунтування зазначеної позиції доцільно звернутися, зокрема, до праць теоретиків права, присвячених дослідженню проблем визначення поняття та сутності інституту права.

Так, П. Рабінович [4] під інститутом права розуміє групу норм права, пов'язаних предметно-функціональними зв'язками, що регулюють конкретний вид суспільних відносин і набувають відносної стійкості та самостійності функціонування. У праці [4] також зазначено, що міжгалузеві інститути регулюють відносини, що належать одночасно до кількох галузей права [4, с. 129]. Водночас О. Балинська зазначає, що сукупність норм у структурі правових інститутів регулює суспільні відносини, що мають відносну самостійність, та звертає увагу на те, що ознакою, яка відрізняє інститут права від галузі чи підгалузі, є масштаб предмета правового регулювання, де інститут права впорядковує лише різні сторони однієї чи вузької групи типових суспільних відносин [5, с. 105].

Л. Коваленко визначає поняття інституту інформаційного права як відносно стійку та визнану групу інформаційно-правових норм, що регулюють певні види інформаційних правовідносин [6, с. 14].

Поряд з тим, О. Ярема дотримується думки, що в сучасній системі права правовий інститут найчастіше виступає у вигляді невеликої спільності правових норм, специфіка яких відноситься до однієї галузі права [7, с. 19]. У той же час міжгалузеві інститути містять норми, які характерні для різних галузей права [7]. Це обумовлюється тим, що в будь-яких однорідних суспільних відносинах одночасно існує кілька інших відносин, відмінних за формою, проте пов'язаних за призначенням.

У даний час правові норми, пов'язані з регулюванням суспільних

відносин щодо протидії використанню ІКТ у терористичних цілях, містяться не тільки в системі інформаційного права, а й у інших галузях права – адміністративному, кримінальному, фінансовому та міжнародному. Інститут протидії використанню ІКТ у терористичних цілях можна віднести до комплексних міжгалузевих правових інститутів.

Наприклад, правові норми, спрямовані на регулювання міжнародних відносин щодо протидії використанню ІКТ з метою терористичної діяльності, містяться у різних міжнародних багатосторонніх та двосторонніх угодах Європейського Союзу (далі – ЄС) та НАТО [8].

Серед нормативно-правових актів України, які регулюють питання протидії загрозам використання ІКТ у терористичних цілях, необхідно виділити Закон України «Про боротьбу з тероризмом» від 20.03.2003 р. № 638-IV (із змінами), який до терористичної діяльності також відносить інформаційну допомогу в плануванні, підготовці або реалізації терористичного акту, пропаганду ідей, поширення матеріалів або інформації, що закликають до здійснення терористичних актів або обґрунтовують чи виправдовують необхідність такої діяльності [9].

Ці ознаки терористичної діяльності мають безпосереднє відношення до використання мережі Інтернет. Відповідно до Закону України «Про медіа» від 13.12.2022 р. № 2849-IX (із змінами), власникам інформаційних ресурсів новин у мережі Інтернет, ресурсів для створення і поширення аудіовізуальних творів заборонено поширювати матеріали, що містять заклики або виправдовують тероризм [10].

Аналогічні вимоги встановлені Законом України «Про медіа» [10] при поширенні інформації в соціальних мережах, а також для власників сервісів розміщення оголошень. Законом [10] також передбачено порядок обмеження доступу до інформації, що містить хибні повідомлення про терористичні

акти, або обґрунтування та виправдання провадження терористичної діяльності.

Згідно з положеннями ст. 258-2 Кримінального кодексу України (далі – КК України) від 05.04.2001 р. № 2341-III (із змінами) [11], за здійснення публічних закликів до терористичної діяльності, за виправдання чи пропаганду тероризму за допомогою засобів масової інформації або інформаційно-телекомунікаційних мереж, включаючи мережу Інтернет, передбачено кримінальне покарання. У зазначеній статті КК України [11] під публічним виправданням тероризму розуміється заява про визнання терористичної ідеології та діяльності доцільними, які можна підтримувати і наслідувати, а під пропагандою тероризму – діяльність з поширення матеріалів та інформації, спрямованих на формування у особи ідеології тероризму, переконання в її привабливості чи сприйняття допустимості здійснення терористичної діяльності.

Водночас Верховний Суд у Огляді судової практики Касаційного кримінального суду у складі Верховного Суду у кримінальних провадженнях щодо кримінальних правопорушень терористичної спрямованості, з метою забезпечення одноманітності судової практики, під публічними закликами до здійснення терористичної діяльності (тобто скоєння злочинів, передбачених статтями 258 – 258-5 КК України [11]) розуміє звернення до інших осіб з метою втягнення їх у вчинення терористичного акту або сприяння до здійснення терористичної діяльності. Звернення може бути виражене у різній формі, у тому числі з використанням технічних засобів [12].

Проведений аналіз підтверджує, що норми, які регулюють суспільні відносини щодо протидії використанню ІКТ у терористичних цілях, містяться в різних міжнародних та національних актах України. Проте у законодавстві України відсутні уніфіковані підходи. Звідси очевидно, що з метою розробки

єдиної концепції побудови системи правового забезпечення протидії використанню ІКТ у терористичних цілях, основу якої мають скласти уніфіковані підходи до подальшого розвитку системи, відповідну сукупність норм слід виділяти як відокремлений інститут інформаційного права, враховуючи адаптацію законодавства України до вимог та рекомендацій ЄС і НАТО.

Цифрова трансформація державного та місцевого управління, економіки та соціальної сфери ставить перед державою завдання, пов'язані із забезпеченням безпеки держави та суспільства, включаючи безпеку інформаційну. В умовах геополітичної обстановки, що змінюється, формування рішень з питань боротьби з російським тероризмом в інформаційній сфері повинно мати пріоритет, а в правовому полі слід приділяти більше уваги протидії використанню новітніх інформаційно-комунікаційних технологій з терористичною метою.

З урахуванням зазначених пріоритетів найближчим часом необхідно розглянути питання оновлення системи правового забезпечення протидії використанню ІКТ у терористичних цілях, а також побудови комплексної ефективної правової системи такої протидії в різних суспільних сферах. Водночас окремі вчені наголошують, що система інформаційного права охоплює різноманітне коло об'єктів інформаційної сфери, серед яких не всі проблеми законодавчо врегульовані, що потребує вдосконалення та розвитку діючих інформаційно-правових інститутів.

Наприклад, це стосується формування нової галузі міжнародного публічного права – міжнародного інформаційного права, в основі якого можна розглядати право інформаційної безпеки. Підтримуючи та розвиваючи зазначений підхід, використання ІКТ з терористичною метою належить до однієї з ключових загроз міжнародній інформаційній безпеці. Це твердження

знайшло відображення в Регламенті Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку), та розглядається в Основах державної політики України в галузі міжнародної інформаційної безпеки [13].

У міжнародних угодах НАТО за участю України міститься сукупність норм, що регулюють відносини протидії застосуванню ІКТ у терористичних цілях. Ці норми слід віднести до структури окремого правового інституту підгалузі інформаційної безпеки галузі інформаційного права.

З'ясовано, що норми, пов'язані з протидією використанню ІКТ у терористичних цілях, повинні знайти відображення у фінансовій сфері. Це насамперед пов'язано з віртуальними активами (криптовалютами), які розвиваються і активно використовуються в злочинній діяльності, та з відсутністю законодавчого регулювання цього явища.

Для довідки: згідно з інформацією Ghost Security Group (GhostSec – організація боротьби з кібертероризмом), міжнародна терористична організація «Ісламська держава Іраку і Леванту» (ІДІЛ, також відома як ІД – «Ісламська держава») використовувала криптовалюту для підтримки своєї діяльності та інших терористичних груп. У ЗМІ зазначалося, що на одному з її рахунків зберігалося біткоїнів на загальну суму 2 млн. дол. США. Можливий обсяг коштів, що зберігається терористичними організаціями в електронних валютах, становить 1–3 % їх загального доходу (4,7–15,6 млн. дол. США).

Нагадаємо, що у 2018 році міжнародна міжурядова організація, яка визначає стандарти та розробляє політику з метою боротьби з відмиванням грошей та фінансуванням тероризму (ФАТФ, англ. FATF), внесла зміни до

Рекомендацій і зробила заяву щодо віртуальних активів, в якій звернула увагу на створення нових можливостей, зокрема для терористичних організацій. Державам було рекомендовано вжити заходів щодо запобігання використанню віртуальних активів терористами. ФАТФ визначила нові поняття, такі як «віртуальні активи» і «провайдери послуг у сфері віртуальних активів», і зазначила, що всі юрисдикції мають вжити законодавчих заходів, спрямованих на запобігання використанню віртуальних активів у протиправних цілях.

В Україні на необхідності правового регулювання криптовалют, у тому числі з метою забезпечення інформаційної безпеки, неодноразово наголошували вчені в галузі інформаційного права. Потреба в адаптації законодавчої бази зумовила розробку низки нормативно-правових актів, які містять принципово нові підходи до впровадження та подальшого регулювання нових об'єктів правовідносин.

17 лютого 2022 року був прийнятий Закон України «Про віртуальні активи», який не набрав чинності, метою якого є законодавче закріплення визначення понять цифрових фінансових активів, цифрової валюти, концепція цифрового гаманця, цифрового запису та цифрової транзакції [14].

Незважаючи на прозорість механізмів, дослідження М. Ільченка «Суб'єкти фінансового моніторингу обігу криптовалюти в Україні та їх повноваження: фінансово-правовий аспект» доводить, що обіг цифрових фінансових активів в Україні, як це передбачено нормативними актами, неможливо відстежити у повному обсязі (зокрема, відповідно до Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06.12.2019 р. № 361-IX, із змінами). Це створює ризики використання цифрової валюти (криптовалюти) у протиправній діяльності [15].

Необхідність правового регулювання питань обороту цифрових валют свідчить про те, що в майбутньому неможливо обійтися без включення до відповідних нормативних актів правових норм, що регулюють протидію використанню криптовалют у протиправних цілях, у тому числі терористичних. Відповідні норми стануть частиною правового інституту протидії використанню ІКТ у терористичних цілях.

Аргументуючи твердження про міжгалузевий характер досліджуваного правового інституту, важливо з'ясувати термін «протидія». Аналіз змісту даної юридичної категорії свідчить, що цей термін включає низку різних заходів правового примусу: захисту, припинення, процесуального забезпечення, безпеки, контролю, нагляду. У зв'язку з цим, для побудови комплексної та ефективної системи протидії використанню ІКТ у терористичних цілях необхідно вжиття перерахованих заходів, що з правової позиції позначиться в адміністративному законодавстві, зважаючи на необхідність розподілу повноважень серед державних органів влади, сил безпеки і оборони, наділення їх новими правами та обов'язками.

Наприклад, з огляду на сучасні терористичні загрози національній безпеці України та актуальні виклики, на виконання ст. 2 Указу Президента України від 05.03.2019 р. № 53/2019 «Про Концепцію боротьби з тероризмом в Україні» [16], Кабінет Міністрів України, за участю Служби безпеки України, Служби зовнішньої розвідки України та Управління державної охорони України (далі – УДО України), розробив та затвердив План заходів з реалізації Концепції боротьби з тероризмом в Україні [17], який враховує організаційні проблеми боротьби з тероризмом, що потребують розв'язання, а також основні пріоритети боротьби з тероризмом, серед яких виділено й аспекти протидії використанню ІКТ у терористичних цілях [16; 17].

В контексті цього нагадаємо, що згідно зі ст. 4 Закону України «Про

боротьбу з тероризмом» [9], головним органом у загальнодержавній системі боротьби з терористичною діяльністю є державний орган спеціального призначення з правоохоронними функціями – Служба безпеки України [9; 18]. Поряд з тим, виходячи з нових викликів та актуальних загроз, тут доцільно також зазначити, що врахування пропозицій УДО України у Плані заходів з реалізації Концепції боротьби з тероризмом в Україні [17], включаючи рекомендації з протидії використанню ІКТ у терористичних цілях, є досить важливим аспектом у боротьбі з тероризмом. Це обумовлено тим, що УДО України як державний правоохоронний орган спеціального призначення, який входить до складу сектору (сил) сектору безпеки і оборони України (згідно зі ст. 12 Закону України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII, із змінами [19]), та відповідно до покладених на нього завдань (визначених Законом України «Про державну охорону органів державної влади України та посадових осіб» від 04.03.1998 р. № 160/98-ВР, із змінами [20]), при здійсненні державної охорони в Україні співпрацює з органами безпеки іноземних держав та бере участь у заходах, спрямованих на боротьбу з тероризмом [20–22]. Також є всі підстави вважати, що сьогодні, враховуючи досвід забезпечення державної охорони, набутого під час війни росії проти України, важливо і потрібно удосконалити механізм взаємодії між УДО України, Службою безпеки України [9; 18; 20; 23] та іншими суб'єктами, які безпосередньо здійснюють боротьбу з тероризмом в Україні (визначених у ст. 4 Закону України «Про боротьбу з тероризмом» [9]), при здійсненні спеціальних операцій УДО України з виявлення та припинення терористичних актів, спрямованих проти посадових осіб та об'єктів, охорону яких доручено підрозділам УДО України і визначено законом, з урахуванням питань протидії використанню ІКТ у терористичних цілях.

Висновки. У зв'язку з агресією росії проти України, вироблення

публічно-правових механізмів на основі дослідження правового регулювання протидії використанню інформаційно-комунікаційних технологій у терористичних цілях, та формування концептуальних науково обґрунтованих міжгалузевих підходів, спрямованих на інтеграцію силових, оперативних та організаційних заходів реагування, є актуальним завданням. Обґрунтованим є висновок про тенденцію до формування міжгалузевого комплексного інституту протидії використанню інформаційно-комунікаційних технологій у терористичних цілях, до структури якого поряд із інформаційно-правовими нормами входять норми різних правових галузей, об'єднані поняттям «інформація», що є базовим у цій сфері.

Комплексний аналіз свідчить, що правові норми, спрямовані на регулювання питань протидії використанню інформаційно-комунікаційних технологій з терористичною метою, містяться у багатосторонніх та двосторонніх міжнародних угодах України з країнами Європейського Союзу та НАТО про співробітництво у сфері забезпечення інформаційної безпеки, а також у базових законах про інформацію, протидію тероризму, спеціальних законах, зокрема у сфері національної безпеки та державної охорони, та у Кримінальному кодексі України. Також актуальним і важливим питанням, враховуючи сучасні загрози та виклики, є удосконалення взаємодії Служби безпеки України та УДО України у забезпеченні національної безпеки України.

Подальші наукові дослідження повинні охоплювати необхідність удосконалення та розвитку національної системи документів стратегічного планування у сфері забезпечення інформаційної безпеки та протидії тероризму відповідно до стандартів Європейського Союзу та НАТО.

Література

1. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 20.08.2024).

2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки України»: Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 20.08.2024).

3. Бліхар М., Мельник Ю. Правові засади інформаційної протидії в умовах воєнного стану. *Аналітично-порівняльне правознавство*. 2023. № 5. С. 306–310. doi: https://doi.org/10.24144/2788-6018.2023.05.55.

4. Рабінович П. М. *Основи теорії та філософії права*. Львів: Видавництво ЛОБФ «Медицина і право», 2021. 256 с.

5. *Проблеми тлумачення правових норм* / Автор-упорядник О. М. Балинська. Львів: Львівський державний університет внутрішніх справ, 2021. 392 с.

6. *Інформаційне право* / За заг. ред. Л. П. Коваленко. Запоріжжя: Видавничий дім «Гельветика» 2022. 284 с.

7. Ковалів М. В., Єсімов С. С., Ярема О. Г. *Інформаційне право України*. Львів: Львівський державний університет внутрішніх справ, 2022. 416 с.

8. Про ратифікацію Додаткового протоколу до Конвенції Ради Європи про запобігання тероризму: Закон України від 20.09.2022 р. № 2589-IX. URL: https://zakon.rada.gov.ua/laws/show/2589-20#Text (дата звернення: 20.08.2024).

9. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. № 638-IV (із змінами). URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата

звернення: 20.08.2024).

10. Про медіа: Закон України від 13.12.2022 р. № 2849-IX (із змінами). URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 20.08.2024).

11. Кримінальний кодекс України: Кодекс України від 05.04.2001 р. № 2341-III (із змінами). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 20.08.2024).

12. *Огляд судової практики Касаційного кримінального суду у складі Верховного Суду у кримінальних провадженнях щодо кримінальних правопорушень терористичної спрямованості. Рішення, внесені до ЄДРСР, за період з 2018 року по червень 2021 року* / Упоряд. заступник голови Касаційного кримінального суду у складі Верховного Суду, канд. юрид. наук В. В. Щепоткіна, правове управління (III) департаменту аналітичної та правової роботи апарату Верховного Суду. Київ, 2021. 29 с. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Oglyad_KKS_06_12_2021.pdf (дата звернення: 20.08.2024).

13. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку). URL: https://zakon.rada.gov.ua/laws/show/984_024-19#Text (дата звернення: 20.08.2024).

14. Про віртуальні активи: Закон України від 17.02.2022 р. № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text (дата звернення: 20.08.2024).

15. Ільченко М. Г. Суб'єкти фінансового моніторингу обігу

криптовалюти в Україні та їх повноваження: фінансово-правовий аспект. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2024. Вип. 81, Ч. 2. С. 149–154. doi: https://doi.org/10.24144/2307-3322.2024.81.2.23.

16. Про Концепцію боротьби з тероризмом в Україні: Указ Президента України від 05.03.2019 р. № 53/2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019#n6 (дата звернення: 20.08.2024).

17. Про затвердження плану заходів з реалізації Концепції боротьби з тероризмом в Україні: Розпорядження Кабінету Міністрів України від 05.01.2021 р. № 7-р. URL: https://zakon.rada.gov.ua/laws/show/7-2021-%D1%80#Text (дата звернення: 20.08.2024).

18. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII (із змінами). URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 20.08.2024).

19. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII (із змінами). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 20.08.2024).

20. Про державну охорону органів державної влади України та посадових осіб: Закон України від 04.03.1998 р. № 160/98-ВР (із змінами). URL: https://zakon.rada.gov.ua/laws/show/160/98-вр#Text (дата звернення: 20.08.2024).

21. Інструкція з організації та порядку дій Управління державної охорони України за рівнями терористичних загроз: Затверджено Наказом Управління державної охорони від 30.06.2016 р. № 185 (із змінами). URL: https://zakon.rada.gov.ua/laws/show/z1037-16#Text (дата звернення: 20.08.2024).

22. Микитюк М. А. *Державна охорона в Україні: адміністративно-правове регулювання*: монографія. Львів. Видавництво Львівської політехніки.

2018. 472 с.

23. Шепель Л. М. Взаємодія Служби безпеки України та УДО у забезпеченні національної безпеки України. *Стан та перспективи реформування сектору безпеки і оборони України*: Матеріали міжнародної науково-практичної конференції (24 листопада 2017 року): у 2 т. Київ: Національна академія прокуратури України, 2017. Т. 1. С. 457–459.

References

1. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 14.09.2020 r. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (date of access: 20.08.2024).

2. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 28.12.2021 r. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (date of access: 20.08.2024).

3. Blikhar M., Melnyk Yu. Pravovi zasady informatsiinoi protydii v umovakh voiennoho stanu. *Analitychno-porivnialne pravoznavstvo*. 2023. № 5. S. 306–310. doi: https://doi.org/10.24144/2788-6018.2023.05.55.

4. Rabinovych P. M. *Osnovy teorii ta filosofii prava*. Lviv: Vydavnytstvo LOBF «Medytsyna i pravo», 2021. 256 s.

5. *Problemy tlumachennia pravovykh norm* / Avtor-uporiadnyk O. M. Balynska. Lviv: Lvivskyi derzhavnyi universytet vnutrishnikh sprav, 2021. 392 s.

6. *Informatsiine pravo* / Za zah. red. L. P. Kovalenko. Zaporizhzhia: Vydavnychyi dim «Helvetyka» 2022. 284 s.

7. Kovaliv M. V., Yesimov S. S., Yarema O. H. *Informatsiine pravo Ukrainy*. Lviv: Lvivskyi derzhavnyi universytet vnutrishnikh sprav, 2022. 416 s.

8. Pro ratyfikatsiiu Dodatkovoho protokolu do Konventsii Rady Yevropy pro zapobihannia teroryzmu: Zakon Ukrainy vid 20.09.2022 r. № 2589-IX. URL: https://zakon.rada.gov.ua/laws/show/2589-20#Text (date of access: 20.08.2024).

9. Pro borotbu z teroryzmom: Zakon Ukrainy vid 20.03.2003 r. № 638-IV (iz zminamy). URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (date of access: 20.08.2024).

10. Pro media: Zakon Ukrainy vid 13.12.2022 r. № 2849-IX (iz zminamy). URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (date of access: 20.08.2024).

11. Kryminalnyi kodeks Ukrainy: Kodeks Ukrainy vid 05.04.2001 r. № 2341-III (iz zminamy). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (date of access: 20.08.2024).

12. *Ohliad sudovoi praktyky Kasatsiinoho kryminalnoho sudu u skladi Verkhovnoho Sudu u kryminalnykh provadzhenniakh shchodo kryminalnykh pravoporushen terorystychnoi spriamovanosti. Rishennia, vneseni do YeDRSR, za period z 2018 roku po cherven 2021 roku* / Uporiad. zastupnyk holovy Kasatsiinoho kryminalnoho sudu u skladi Verkhovnoho Sudu, kand. yuryd. nauk V. V. Shchepotkina, pravove upravlinnia (III) departamentu analitychnoi ta pravovoi roboty aparatu Verkhovnoho Sudu. Kyiv, 2021. 29 s. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Ogl yad_KKS_06_12_2021.pdf (date of access: 20.08.2024).

13. Rehlament Yevropeiskoho Parlamentu i Rady (IeS) 2019/881 vid 17 kvitnia 2019 roku pro Ahentstvo Yevropeiskoho Soiuzu z pytan merezhevoi ta informatsiinoi bezpeky (ENISA) ta pro sertyfikatsiiu kiberbezpeky informatsiino-komunikatsiinykh tekhnolohii, a takozh pro skasuvannia Rehlamentu (IeS) № 526/2013 (Akt pro kiberbezpeku). URL: https://zakon.rada.gov.ua/laws/show/984_024-19#Text (date of access:

20.08.2024).

14. Pro virtualni aktyvy: Zakon Ukrainy vid 17.02.2022 r. № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text (date of access: 20.08.2024).

15. Ilchenko M. H. Subiekty finansovoho monitorynhu obihu kryptovaliuty v Ukraini ta yikh povnovazhennia: finansovo-pravovyi aspekt. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Ceriia: Pravo*. 2024. Vyp. 81, Ch. 2. S. 149–154. doi: https://doi.org/10.24144/2307-3322.2024.81.2.23.

16. Pro Kontseptsiiu borotby z teroryzmom v Ukraini: Ukaz Prezydenta Ukrainy vid 05.03.2019 r. № 53/2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019#n6 (date of access: 20.08.2024).

17. Pro zatverdzhennia planu zakhodiv z realizatsii Kontseptsii borotby z teroryzmom v Ukraini: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 05.01.2021 r. № 7-p. URL: https://zakon.rada.gov.ua/laws/show/7-2021-%D1%80#Text (date of access: 20.08.2024).

18. Pro Sluzhbu bezpeky Ukrainy: Zakon Ukrainy vid 25.03.1992 r. № 2229-XII (iz zminamy). URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (date of access: 20.08.2024).

19. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018 r. № 2469-VIII (iz zminamy). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (date of access: 20.08.2024).

20. Pro derzhavnu okhoronu orhaniv derzhavnoi vlady Ukrainy ta posadovykh osib: Zakon Ukrainy vid 04.03.1998 r. № 160/98-BP (iz zminamy). URL: https://zakon.rada.gov.ua/laws/show/160/98-вр#Text (date of access: 20.08.2024).

21. Instruktsiia z orhanizatsii ta poriadku dii Upravlinnia derzhavnoi okhorony Ukrainy za rivniamy terorystychnykh zahroz: Zatverdzheno Nakazom Upravlinnia derzhavnoi okhorony vid 30.06.2016 r. № 185 (iz zminamy). URL:

https://zakon.rada.gov.ua/laws/show/z1037-16#Text (date of access: 20.08.2024).

22. Mykytiuk M. A. *Derzhavna okhorona v Ukraini: administratyvno-pravove rehuliuvannia*: monohrafiia. Lviv. Vydavnytstvo Lvivskoi politekhniky. 2018. 472 s.

23. Shepel L. M. Vzaiemodiia Sluzhby bezpeky Ukrainy ta UDO u zabezpechenni natsionalnoi bezpeky Ukrainy. *Stan ta perspektyvy reformuvannia sektoru bezpeky i oborony Ukrainy*: Materialy mizhnarodnoi naukovo-praktychnoi konferentsii (24 lystopada 2017 roku): u 2 t. Kyiv: Natsionalna akademiia prokuratury Ukrainy, 2017. T. 1. S. 457–459.