УДК 32.019.51:323.28:323.2(477)

ПОЛЯКОВ О.М., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
ORCID: https://orcid.org/0000-0002-8984-1476

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО УКРАЇНИ У СФЕРІ БОРОТЬБИ З КІБЕРТЕРОРИЗМОМ

DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346485

Анотація. *У статті розглядаються ключові аспекти міжнародного співробітництва України у сфері протидії кібертероризму в умовах воєнного стану. З урахуванням опрацьованих різноманітних підходів до визначення кібертероризму, вироблених вітчизняними вченими, виділено його основні правові ознаки. На підставі аналізу нормативно-правової бази у сфері забезпечення кібербезпеки визначено основні міжнародні договори України з питань боротьби з кібертероризмом. Розкрито міжнародний механізм боротьби з кіберетроризмом з урахуванням інституційних інструментів ООН, НАТО та ЄС. Досліджено перспективи розвитку міжнародного співробітництва у цій сфері. Результати дослідження свідчать про зростання ролі України у забезпеченні міжнародної кібербезпеки з урахуванням євроінтеграційних процесів.*

Ключові слова: *кібербезпека, кібертероризм, міжнародне співробітництво, ЄС, НАТО.*

Summary*. The article examines key aspects of Ukraine's international cooperation in the field of countering cyberterrorism under martial law. Taking into account various approaches to defining cyberterrorism, its main legal features are highlighted. Based on the analysis of the regulatory framework in the field of ensuring cybersecurity, the main international treaties of Ukraine on combating cyberterrorism are identified. The international mechanism for combating cyberterrorism is disclosed, taking into account the institutional instruments of the UN, NATO and the EU. The prospects for the development of international cooperation in this area are studied. The results of the study indicate the growth of Ukraine's role in ensuring international cybersecurity, taking into account European integration processes.*

Keywords: *cybersecurity, cyberterrorism, international cooperation, EU, NATO.*

Постановка проблеми.

Міжнародна глобалізація сучасного світу, крім позитивного впливу, зумовлює і низку негативних чинників, серед них – збільшення сприятливих можливостей для розвитку кіберзлочинності та її різновидів. Розвиток кібертероризму, його підвищена небезпечність зумовлює необхідність пошуку дієвих шляхів підвищення ефективності міжнародного співробітництва у сфері боротьби з цим негативним явищем, яке набуває дедалі більшої актуальності в сучасному світі, особливо для держав, що стикаються з систематичними кібератаками. Для України, яка з 2014 року є об’єктом кіберагресії з боку рф, протидія кібертероризму є не лише пріоритетом державної політики у сфері забезпечення кібербезпеки, але й елементом міжнародної безпеки. Сьогодні Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така

деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури[1]. Глобального масштабу набуває використання кіберпростору терористичними організаціями. Пріоритетними цілями кібертероризму залишаються об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо[1].

У першій половині 2025 року Україна посіла п'яте місце у світі за кількістю здійснених проти країни кібератак[2].

Результати аналізу наукових публікацій. Теоретичні та інформаційно-правові аспекти кіберетроризму досліджували Р.Банк [3], І.Білан [4], Л.Лабенко [5], Б.Леонов [6], Д.Мельник [7], В.Пилипчук, О.Дзьобань [8] та ін.

Окремі аспекти міжнародного співробітництва у сфері забезпечення кібербезпеки вивчали С.Демедюк [9], М.Сливка[10], О.Поляков[11], Р.Лук'янчук [12] Д.Федченко [13]та ін.

Водночас, малодослідженими залишаються міжнародно-правові механізми боротьби з кібертероризмом в умовах воєнного стану.

Метою статті є визначення на підставі аналізу міжнародних договорів у сфері боротьби з кіберзлочинністю найбільш ефективні форми та механізми боротьби з кібертероризмом.

Виклад основного матеріалу. Сьогодні немає єдиного визначення поняття "кібертероризм". Водночас, у юридичній літературі триває жвава дискусія щодо визначення цього поняття.

Одні автори під кібертероризмом пропонують розуміти навмисну, політично вмотивовану атаку на об'єкти інформаційного простору, що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійснені з метою порушення державної чи громадської безпеки, залякування населення, провокації військового конфлікту чи загроза вчинення таких дій [8].

Інші автори під кібертероризмом пропонують розуміти суспільно небезпечну діяльність, яка полягає у вчиненні за допомогою комп'ютерних та електронних комунікаційних засобів навмисних, політично мотивованих атак на комп'ютерні системи / мережі, на інформацію, що обробляється (циркулює) в них, якщо вони викликають порушення роботи критичної інфраструктури держави та створюють (можуть створювати) небезпеку для життя й здоров'я людей, завдали чи можуть завдати значної шкоди матеріальним об'єктам, або спричинили інші тяжкі наслідки, й були вчинені з метою привернення максимально можливої уваги до політичних вимог терористів або використання кіберпростору для інших цілей терористичної діяльності, безпосередньо не пов'язаних зі здійсненням терактів [7, с. 144-158].

Непоодинокими є спроби покласти в основу кібертероризму кібератаки [4, с. 69].

Така дискусія свідчить про дуалізм думок у науковому світі та наявність проблеми визначення кібертероризму в інформаційному праві.

Не простежується системний підхід до визначення кібертероризму й в чинному законодавстві, де під кібертероризмом розуміється терористична діяльність, що здійснюється в кіберпросторі або з його використанням (ст. 1 Закону України "Про основні засади забезпечення кібербезпеки України") [14].

На нашу думку, серед визначальних ознак кібертероризму доцільно виділити: кібератаки (форми); здійснення в кіберпросторі або з його використанням (просторова дія); організовані хакерські групи та організації (суб'єкти кібертероризму); залякування

населення (спосіб); заподіяння шкоди об'єктам критичної інформаційної інфраструктури або міжнародному правопорядку(терористичні цілі).

Суспільно небезпечні наслідки кібертероризму є доволі масштабними. Це призводить до дестабілізації суспільства, економіки чи критичної інфраструктури.

У юридичній літературі підкреслюється транснаціональний характер кіберзагроз, суспільно небезпечні прояви яких вимагають колективної відповіді міжнародної спільноти, яка зумовлює потребу удосконалення міжнародного співробітництва у сфері забезпечення кібербезпеки.

Міжнародне співробітництво є ключовим елементом у ліквідації правового вакууму, який існує між динамічним розвитком інформаційних технологій та законодавчим реагуванням на сучасні кіберзагрози.

Міжнародне співробітництво здійснюється з метою: зміцнення взаємної довіри у сфері кібербезпеки; вироблення спільних підходів до протидії кіберзагрозам; консолідації зусиль у розслідуванні та запобіганні кіберзлочинам; недопущення використання кіберпростору в протиправних цілях; виконання Україною зобов'язань у рамках, укладених міжнародних договорів у контексті співробітництва у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами і спеціальними службами, а також міжнародними організаціями [11, с. 131].

Міжнародне співробітництво у сфері боротьби з тероризмом, як правило, відбувається шляхом: 1) встановлення на міжнародному рівні єдиних підходів щодо притягнення до кримінальної відповідальності за такий вид тероризму; 2) розробки та укладання міжнародних договорів у сфері боротьби з тероризмом, прийняття інших міжнародних документів як правової основи регулювання діяльності держав, міжнародних організацій у цій сфері [15, с. 314].

Аналіз наявних міжнародних антитерористичних структур, які займаються запобіганням різних видів тероризму, дозволяє констатувати, що існує міжнародний (інтернаціональний) та регіональний (субрегіональний) рівень організації відповідного співробітництва держав у цій сфері.

На міжнародному рівні головним органом є ООН, на яку покладено здійснення єдиної антизлочинної політики у світі. Це єдина з існуючих організацій, що володіє мандатом та міжнародним механізмом, необхідним для надання країнам ефективної допомоги з метою запобігання злочинності та боротьби з нею у національному та міжнародному масштабах [15, с. 315].

У системі органів ООН функціонують Генеральна Асамблея, Секретаріат, а також спеціалізовані органи та установи – Міжнародна організація цивільної авіації (ІКАО), Міжнародна морська організація (ІМО), Міжнародна агенція з атомної енергетики (МАГАТЕ), які беруть участь у міжнародному співробітництві сфери боротьби з тероризмом. Слід також виділити діяльність спеціальних доповідачів ООН. Одним із важливих механізмів міжнародного співробітництва щодо боротьби з тероризмом стало створення на підставі Резолюції Ради Безпеки ООН 1373 (2001) Контртерористичного комітету (КТК), до складу якого увійшли члени Ради Безпеки ООН. Серед тенденцій розвитку КТК відзначають: його потенціал як ключового міжнародного інституціонального антитерористичного органу; спрямованість до універсалізації системи в цілому; чіткі й транспарентні механізми його діяльності [16, с. 239].

ООН підтримує тісне співробітництво з регіональними організаціями, наприклад ЄС, ОБСЄ, НАТО.

ОБСЄ як регіональна міжурядова організація, яка займається питаннями колективної безпеки, виробила низку політичних обов'язків у сфері боротьби з

тероризмом. Одним із яких є покладення на держав-учасниць зобов'язань ратифікувати всі конвенції і протоколи ООН у сфері боротьби з тероризмом.

Реалізація політики ЄС у сфері боротьби з тероризмом проводиться через формування співробітництва правоохоронних органів і спеціальних служб європейських країн, утворення наднаціональних структур, таких як Євроюст, Європол, а також взаємодії з ООН, регіональними, субрегіональними структурами у цій сфері [15, с. 323].

Серед органів, які здійснюють регулювання кіберпростору, варто зазначити такі: у Європейському Союзі функціонує Агентство з мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA), у Сполучених Штатах Америки кібербезпекою займається Агентство Національної Безпеки, у НАТО створений Комітет з кібернетичної оборони (The Cyber Defence Committee), а також Спільний центр з кібернетичної оборони (Cooperative Cyber Defence Centreof Excellence), Спеціалізований центр з оборони в сфері кібербезпеки НАТО (CCDCOE), Міжнародний альянс із забезпечення кібербезпеки (ICSPA), Інтерпол (INTERPOL), Міжнародне багатостороннє товариство проти кіберзагроз (IMPACT) та ін. [13, с. 655].

Відносини України з НАТО, які розпочалися з підписання ще у 1994 році програми співробітництва "Партнерство заради миру", дедалі зміцнюються. У липні 1997 р. в Мадриді було підписано "Хартію про особливе партнерство між Україною і НАТО". Відповідно до цієї Хартії була утворена Комісія Україна-НАТО.

Річні національні програми під егідою Комісії Україна-НАТО є основним механізмом співробітництва України з НАТО. Це співробітництво охоплює операції з підтримання миру, реформування структур безпеки і оборони, безпосереднє військове співробітництво, оборонні технології та ін. Одним із основних питань міжнародного співробітництва є забезпечення Україною взаємосумісності та узгодженості із стандартами НАТО, у т.ч. у сфері кіберебзпеки.

Крім цих програмних документів, правову базу співробітництва у сфері боротьби з кібетероризмом складають: Закон України "Про основні засади забезпечення кібербезпеки України", Конвенція про кіберзлочинність 2001 р. (Будапештська конвенція), Стратегія ЄС для цифрового десятиліття 2020 р., інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Серед пріоритетних міжнародних зобов'язань України слід виділити обов'язок щодо імплементації Директиви 2016/1148 про безпеку мережевих та інформаційних систем (NIS Directive) [17], яка запровадила нову культуру кібербезпеки в ЄС, зміст якої підтримує і полегшує стратегічне співробітництво і обмін інформацією між державами-членами ЄС. З 18 жовтня 2024 року набула чинності нова директива ЄС із кібербезпеки — Директива NIS 2 "Мережева та інформаційна безпека" (NIS 2 Directive) [18], яка встановлює більш суворі правила кібербезпеки для своїх держав-членів.

Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки, зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України "Про порядок направлення підрозділів Збройних Сил України до інших держав" та "Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України" [14].

У 2023 році був запроваджений за участю 11 країн (включаючи Україну, США, Великобританію) Талліннський механізм, який передбачає підтримку стійкості цивільної інфраструктури України перед кіберзагрозами та координацію надання кібердопомоги за трьома напрямками: 1) короткострокова підтримка,

2) середньострокове нарощування та 3) довгострокова кіберстійкість. Цей механізм доповнює зусилля із забезпечення кіберебезпеки шляхом залученням приватного сектору для захисту критичної інфраструктури. У 2024–2025 роках Талліннський механізм допомагав координувати відповідь на кібератаки проти енергосистеми України шляхом обміну аналітичним даними з Агентством Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), об'єднанням зусиль експертів для обговорення приватно-державного партнерства у цій сфері з урахуванням загальновизнаних засад забезпечення кібербезпеки.

У Законі України "Про основні засади забезпечення кібербезпеки України" серед принципів забезпечення кбербезпеки виділяються принципи пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам; реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі; міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам; консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях [14].

Не менш важливим є також проголошений законом принцип пріоритетності дії міжнародних договорів над національним законодавством. Так, у ч. 2 ст. 3 Закону "Про основні засади забезпечення кібербезпеки України" передбачено, якщо міжнародним договором України, згоду на обов'язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені цим Законом, застосовуються положення міжнародного договору України [14].

У ст. 14 Закону України "Про основні засади забезпечення кібербезпеки України" [14] регламентовано, що Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю. Відповідно до законодавства України у сфері зовнішніх зносин суб'єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі [14].

Співробітництво України з іншими державами світу у сфері забезпечення кібербезпеки може здійснюватись шляхом: 1) взаємодії на міжнародному рівні при протидії кіберзагрозам та кібератакам; 2) обміну досвідом побудови та функціонування національних систем кібербезпеки; 3) вироблення стандартів кібербезпеки [19, с. 16]. Інформацію з питань, пов'язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору (ч. 4 ст. 15 Закону "Про основні засади забезпечення кібербезпеки України") [14].

Як ми бачимо, багаторівневе міжнародне співробітництво у сфері забезпечення кібербезпеки є важливим компонентом для безпосередньої протидії кібертакам, підтримуваними державою-терористом.

Не випадково, однією з важливих складових національної системи реагування на кіберінциденти, кібератаки, кіберзагрози визнано взаємодію з іноземними та

міжнародними організаціями з питань реагування на кіберінциденти, кібератаки, кіберзагрози, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST (ч. 3 ст. 9 Закону) [14].

Такі засади взаємодії покладено в основу формування Стратегії кібербезпеки України (далі – Стратегія), яка враховує стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав - членів ЄС та держав - членів НАТО.

Зокрема, цією Стратегією проголошено, що для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є:

посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування);

забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами-членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія) [1].

Передбачається, що для досягнення цілі С.1 “Дієва кіберборона” Україна сформує систему дієвої кібероборони шляхом:

запровадження ефективних механізмів взаємодії основних суб’єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони;

проведення щонайменше двічі на рік спільних тематичних навчань із відповідними підрозділами держав - членів НАТО задля досягнення оперативної сумісності[1].

Стратегія проголошує найважливішим напрямком зовнішньополітичної діяльності України у сфері кібербезпеки забезпечення поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі. В цьому контексті Україна приділятиме особливу увагу спільній з партнерами протидії міжнародному тероризму, виявленню, попередженню і припиненню розвиватиме на договірній основі з партнерськими спецслужбами держав-членів ЄС і держав-членів НАТО взаємовигідний обмін інформацією та досвідом щодо забезпечення національної безпеки у кіберпросторі, використовуватиме кращі світові практики, активно здійснюватиме інші спільні заходи, що сприятимуть зміцненню наукової, матеріально-технічної бази та кадрового потенціалу у сфері кібербезпеки [1].

Серед асиметричних інструментів кіберстримування виділено налагодження систематичного обміну інформацією про деструктивну діяльність у кіберпросторі з Сполученими Штатами Америки, державами - членами ЄС та державами - членами НАТО, створення платформи такого обміну [1]. На нашу думку, такі інструменти є важливою складовою запобігання кібертероризму.

Відзначимо, що викладеними заходами не вичерпується державна політика у сфері боротьби з кібертероризмом. Політика більшості провідних країн світу виходить із необхідності створення комплексної системи протидії тероризму з боку світової

спільноти, що включає: удосконалення нормативно-правової бази з питань боротьби з кібертероризмом; посилення взаємодії міждержавних органів, надання допомоги та сприяння в боротьбі з тероризмом; налагодження співпраці оперативних та розвідувальних органів; максимальний тиск на країни, які підтримують тероризм, використовуючи комплексні засоби протидії, в тому числі й військові; відмова в задоволенні вимог терористів; активізація діяльності силових структур; формування підрозділів боротьби з кібертероризмом та інші заходи [20, с. 27-28].

Висновки. Міжнародне співробітництво у сфері боротьби з кібертероризмом можна визначити як об'єднання зусиль міжнародної спільноти, правоохоронних органів та спеціальних служб різних країн, спрямованих на запобігання, припинення, виявлення терористичної діяльності, що здійснюється в кіберпросторі або з його використанням, шляхом укладання міжнародних угод, а також удосконалення координації та взаємодії у сфері забезпечення кібербезпеки. Основні форми такого співробітництва передбачають договірні та інституційні механізми, участь у міжнародних форумах та об'єднаннях держав для забезпечення кібербезпеки.

Ключовим напрямком зовнішньополітичної діяльності України є: розвиток активної співпраця у сфері кібербезпеки з іноземними партнерами (Сполученими Штатами Америки, Сполученим Королівством Великої Британії і Північної Ірландії, Федеративною Республікою Німеччина тощо), поглиблення співробітництва з ЄС та НАТО шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України, розвиток і вдосконалення договірно-правової бази, що регламентує міжнародне співробітництво у сфері боротьби з кібертероризмом, зміцнення спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Використана література

1. Стратегія кібербезпеки України: затвердж. Указом Президента України від 26.08.2021 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

2. Україна посіла п'яте місце у світі за кількістю кібератак проти країни – Microsoft URL: https://bukvy.org/ukrayina-posila-p-yate-mistse-u-sviti-za-kilkistyu-kiberatak-proty-krayiny-microsoft/

3. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право*. 2016. № 1(16)/2016. С. 110-116.

4. Білан І.А. Кібертероризм: інформаційно-правовий аспект. *Інформація і право.* 2023. № 4(47)/2023. С. 64-74.

5. Лабенко Л.В. Інформаційний тероризм: поняття та ознаки. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/3439.

6. Леонов Б.Д. Тероризм: інформаційно-правовий вимір. *Інформація і право*. 2021. №2(37)/2021. С. 72-79.

7. Мельник Д.С. Кібертероризм: поняття, форми прояву, перспективні заходи протидії. *Вісник Харківського національного університету внутрішніх справ.* Харків, 2023. № 3 (102). С. 144-158.

8. Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети*. 2011. № 4. С. 12-17.

9. Демедюк С.В. Окремі питання адміністративно-правового та організаційного забезпечення кібербезпеки. *Південноукраїнський правничий часопис*. 2015. № 2. С. 144–147.

10. Сливка М.М. Міжнародне співробітництво у сфері забезпечення кібербезпеки України. *Юридичний науковий електронний журнал*. 2022. № 10/2022. С. 489-491.

11. Поляков О.М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2 (37). С. 129–138.

12. Лук'янчук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник Національної академії державного управління при Президентові України*. Серія : Державне управління. 2015. № 4. С. 50-56.

13. Федченко Д.І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. *Молодий вчений*. 2017. Випуск 5 (57). С. 653–658.

14. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. №2163-VIII. *Відомості Верховної Ради України.* 2017. №45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

15. Леонов Б.Д. Запобігання тероризму: кримінологічний аспект: моногр. К.: Видавничий дім «АртЕк», 2015. 435 с.

16. Антипенко В.Ф. Оптимізація антитерористичної системи держави в умовах міжнародної і регіональної інтеграції. К., 2008. 405 с.

17. Директива Європейського Парламенту (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text.

18. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

19. Артеменко Я.В. Адміністративно-правове забезпечення функціонування національної системи кібербезпеки України: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ, 2020. 21 с.

20. Бердюк В.І., Погорецький М.А. Міжнародне співробітництво у сфері протидії тероризму. *Боротьба з організованою злочинністю і корупцією (теорія і практика*). 2009. №21. С. 27-28.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~