УДК 341
DOI https://doi.org/10.24144/2307-3322.2026.93.5.52

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА МІЖНАРОДНОЇ СИСТЕМИ ПРОТИДІЇ ТЕРОРИЗМУ

Онищенко О.В.,
аспірант кафедри міжнародного та європейського права
факультету права та міжнародних відносин
Державного некомерційного підприємства
«Державний університет «Київський авіаційний інститут»
ORCID: 0009-0009-9376-0078

Онищенко О.В. Інформаційна безпека як складова міжнародної системи протидії тероризму.

У статті досліджується роль інформаційної безпеки в системі міжнародного співробітництва у сфері протидії тероризму, що набуває особливого значення в умовах стрімкого розвитку цифрових технологій, глобалізації комунікативних процесів та зростання частоти кібератак на критичну інфраструктуру держав і міжнародних організацій. Актуальність теми зумовлена трансформацією терористичної діяльності під впливом цифровізації: терористичні мережі дедалі активніше використовують кіберпростір як середовище для планування, координації та здійснення атак, що суттєво ускладнює традиційні підходи до боротьби із цими явищами.

Проаналізовано основні загрози, що виникають унаслідок використання терористичними організаціями інформаційно-комунікаційних технологій (ІКТ) для координації діяльності, планування та здійснення атак, вербування прихильників, поширення радикальної пропаганди та цілеспрямованої маніпуляції суспільною думкою. Встановлено, що анонімність, транскордонність і висока швидкість поширення інформації в кіберпросторі суттєво посилюють деструктивний потенціал терористичних структур, ускладнюють їх ідентифікацію та нейтралізацію з боку правоохоронних органів.

Розглянуто механізми міжнародної співпраці у сфері кібербезпеки, включно з діяльністю ООН, НАТО, Європолу та Глобального інтернет-форуму з протидії тероризму (GIFCT). Детально проаналізовано досвід США, Ізраїлю, країн Європейського Союзу та України у формуванні та вдосконаленні національних систем кіберзахисту, виявлено спільні закономірності й специфічні особливості їхніх підходів в умовах різних безпекових середовищ.

Запропоновано комплекс заходів щодо посилення інформаційної складової антитерористичної діяльності: вдосконалення правового регулювання кіберпростору, гармонізація національного законодавства з міжнародними стандартами та нормами, створення ефективних систем раннього виявлення й нейтралізації кіберзагроз, протидія онлайн-радикалізації та підвищення цифрової грамотності населення. Обґрунтовано необхідність комплексного міждисциплінарного підходу, що органічно поєднує правові, організаційні, освітні та технологічні інструменти задля зміцнення глобальної інформаційної безпеки й підвищення стійкості суспільства перед сучасними терористичними викликами.

Ключові слова: інформаційна безпека, міжнародний тероризм, кібертероризм, інформаційно-комунікаційні технології, кібератаки, міжнародна співпраця, онлайн-радикалізація, протидія тероризму, гібридна війна.

Onyshchenko O.V. Information security as a component of the international counterterrorism system.

The article examines the role of information security in the system of international cooperation in the field of counterterrorism, which is becoming particularly important in the context of the rapid development of digital technologies, globalization of communication processes, and the increasing frequency of cyberattacks on the critical infrastructure of states and international organizations. The relevance of

the topic is due to the transformation of terrorist activity under the influence of digitalization: terrorist networks are increasingly using cyberspace as an environment for planning, coordinating, and carrying out attacks, which significantly complicates traditional approaches to combating these phenomena.

The main threats arising from the use of information and communication technologies (ICT) by terrorist organizations to coordinate activities, plan and carry out attacks, recruit supporters, spread radical propaganda, and deliberately manipulate public opinion are analyzed. It has been established that anonymity, cross-border nature, and high speed of information dissemination in cyberspace significantly increase the destructive potential of terrorist structures and complicate their identification and neutralization by law enforcement agencies.

The mechanisms of international cooperation in the field of cybersecurity are considered, including the activities of the UN, NATO, Europol, and the Global Internet Forum to Counter Terrorism (GIFCT). The experience of the United States, Israel, European Union countries, and Ukraine in forming and improving national cyber defense systems is analyzed in detail, and common patterns and specific features of their approaches in different security environments are identified.

A set of measures has been proposed to strengthen the information component of counterterrorism activities: improving the legal regulation of cyberspace, harmonizing national legislation with international standards and norms, creating effective systems for early detection and neutralization of cyber threats, countering online radicalization, and improving the digital literacy of the population. The need for a comprehensive interdisciplinary approach that organically combines legal, organizational, educational, and technological tools to strengthen global information security and increase the resilience of society to modern terrorist challenges has been substantiated.

Key words: information security, international terrorism, cyberterrorism, information and communication technologies, cyberattacks, international cooperation, online radicalization, counterterrorism, hybrid warfare.

Постановка проблеми. В умовах глобальних викликів цифрової трансформації суспільства інформаційна безпека набуває принципово нового виміру, виступаючи не лише технічною, але й геополітичною категорією. Стрімкий розвиток інформаційно-комунікаційних технологій (ІКТ) відкрив для терористичних організацій якісно нові можливості для конспіративної діяльності, пропаганди, вербування та координації дій [1]. Водночас цифровий простір перетворився на самостійне поле протиборства між державними структурами і недержавними деструктивними акторами.

Проблематика дослідження перебуває на перетині кількох системних викликів, що детермінують складність і багатовимірність розглянутого феномену. По-перше, широке застосування терористами шифрованих комунікаційних каналів істотно унеможливлює своєчасний моніторинг інформаційних потоків та превентивне реагування з боку спеціальних служб, що суттєво знижує ефективність контртерористичних заходів [2]. По-друге, платформи соціальних медіа функціонують як інструмент масштабної онлайн-радикалізації соціально вразливих груп населення – передусім молоді, – що зумовлює необхідність розробки цілеспрямованих механізмів превентивного впливу [3]. По-третє, кібертерористичні атаки на об'єкти критичної інфраструктури – енергетичного, транспортного, медичного та фінансового секторів – становлять безпосередню й системну загрозу національній безпеці держав, здатну спричинити каскадні наслідки для стабільності суспільних інститутів [4]. По-четверте, відсутність дієвих механізмів міжнародної координації у сфері кібербезпеки, детермінована сукупністю правових колізій, інституційних обмежень та геополітичних суперечностей, суттєво редукує потенціал спільного реагування на транснаціональні терористичні загрози [5]. По-п'яте, забезпечення збалансованого співвідношення між імперативами національної безпеки та захистом фундаментальних прав людини – зокрема права на приватність і свободи вираження поглядів – залишається предметом гострих дискусій у правовій, політологічній та етичній площинах [6]. Комплексне вирішення зазначених проблем передбачає синтез технологічних, правових та організаційних механізмів, що й обумовлює актуальність і практичну значущість наукової статті.

Мета дослідження полягає у всебічному аналізі ролі інформаційної безпеки в міжнародній системі протидії тероризму та визначенні пріоритетних напрямів удосконалення антитерористичної діяльності в інформаційному просторі в умовах цифровізації глобальних комунікацій.

Для досягнення поставленої мети вирішувалися такі **завдання:** дослідити сучасні загрози інформаційної безпеки, пов'язані з терористичною діяльністю; проаналізувати механізми міжна-

родної співпраці у сфері інформаційної протидії тероризму; вивчити досвід провідних країн у забезпеченні кібербезпеки в контексті антитерористичної діяльності; виявити основні проблеми і виклики у цій сфері; сформулювати науково обґрунтовані рекомендації щодо підвищення ефективності інформаційної складової для міжнародного співробітництва у сфері протидії тероризму.

Стан опрацювання проблематики. Науковий дискурс щодо проблематики інформаційної безпеки в антитерористичному вимірі вирізняється високим рівнем міждисциплінарності та концептуальної різноманітності, поєднуючи напрацювання у сфері безпекових студій, міжнародних відносин, кібернетики, права, комунікацій та соціальної психології. Системний аналіз зазначеної тематики засвідчує поступову трансформацію підходів – від традиційного розуміння тероризму до усвідомлення його інформаційно-мережевої природи в умовах цифрової глобалізації.

Серед зарубіжних дослідників вагоме місце посідають праці Bruce Hoffman, який здійснив комплексний аналіз еволюції тероризму, акцентуючи увагу на його адаптації до цифрового середовища та використанні інформаційних технологій як інструменту стратегічного впливу. У його дослідженнях обґрунтовується теза про трансформацію організаційних моделей терористичних структур у напрямі мережевої децентралізації, що безпосередньо впливає на характер інформаційних загроз [7].

Фундаментальний внесок у розроблення концепції кібертероризму зробила Dorothy Denning, яка сформулювала теоретичні засади розмежування кібертероризму, кіберзлочинності та інформаційної війни. Її підхід дозволив окреслити критерії кваліфікації кібератак як терористичних актів та визначити їх потенційний вплив на критичну інфраструктуру і національну безпеку [8].

Значну увагу технологічним та ідеологічним аспектам використання мережевих платформ терористичними організаціями приділив Gabriel Weimann. У його працях Інтернет розглядається як багатофункціональний інструмент – для пропаганди, рекрутингу, координації діяльності та фінансування, що формує новий вимір інформаційно-психологічного впливу [9].

Теоретичне осмислення інформаційних операцій та дезінформаційних стратегій у контексті безпекових загроз ґрунтовно розробив Thomas Rid, який довів, що сучасні інформаційні кампанії мають ознаки складних політико-комунікативних операцій і можуть функціонувати як інструмент гібридного протистояння [10]. У свою чергу, Ben Buchanan дослідив роль кіберзасобів у геополітичному суперництві держав, акцентуючи на стратегічному значенні кібероперацій як елементу стримування та примусу [11].

Отже, сучасна наукова розробленість проблематики інформаційної безпеки в антитерористичному контексті демонструє перехід від фрагментарного аналізу окремих явищ до формування комплексної теоретико-методологічної парадигми, що інтегрує технологічний, правовий, політичний та соціально-психологічний виміри.

Серед вітчизняних науковців помітний внесок у дослідження питань інформаційної безпеки та кібертероризму зробили О. Баранов, М. Гуцалюк, О. Довгань, С. Єсімов, Т. Ткачук [12]. Нормативно-аналітичний вимір проблеми відображено в документах міжнародних організацій – ООН, НАТО, Європолу, ОБСЄ, – а також у Резолюції Ради Безпеки ООН 2341 (2017), яка визнала критичну важливість захисту інфраструктури від кібератак [13].

Разом із тим, динамічний характер еволюції технологій і терористичних загроз обумовлює необхідність подальших досліджень, орієнтованих на розробку адаптивних механізмів забезпечення інформаційної безпеки в антитерористичній діяльності.

Виклад основного матеріалу. Інформаційна безпека являє собою стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання та розвиток в інтересах громадян, організацій і держави [14]. У контексті протидії тероризму вона набуває подвійного значення: виступає одночасно об’єктом захисту та інструментом активної антитерористичної боротьби. Концептуальним підґрунтям інформаційної безпеки слугує тріада CIA (Confidentiality – конфіденційність, Integrity – цілісність, Availability – доступність) [15]. Терористичні організації системно намагаються порушити всі три складові: атакуючи критичну інфраструктуру (порушення доступності), поширюючи дезінформацію (порушення цілісності) або викрадаючи конфіденційні дані (порушення конфіденційності). Це перетворює кіберпростір на самостійний операційний вимір терористичної активності, що потребує розробки специфічних інституційних, правових і технологічних інструментів протидії.

Усвідомлення концептуальних засад дозволяє перейти до аналізу конкретних типів загроз, які генерує сучасний тероризм в інформаційному просторі. Широке й диверсифіковане використання

ІКТ терористичними організаціями охоплює кілька взаємопов'язаних напрямів. Кібертероризм як самостійна форма терористичної діяльності передбачає використання комп'ютерних систем, мереж і даних як безпосередніх об'єктів і засобів атаки [16]. Критична інфраструктура держав – енергетичні системи, водопостачання, транспорт, фінансові установи, урядові мережі та медичні заклади – є пріоритетними цілями кібертерористів. Показовим прикладом є атаки групи хакерів Sandworm на електромережі України у 2015–2016 рр., що залишили без електропостачання сотні тисяч мирних мешканців [17]. Ці події стали першим у світі підтвердженим прикладом деструктивної кібератаки на об'єкти цивільної інфраструктури.

Паралельно з безпосередніми кібератаками терористичні організації активно використовують онлайн-середовище для пропаганди і вербування. Соціальні мережі, відеохостингові платформи та месенджери слугують інструментом поширення пропагандистських матеріалів, залучення та радикалізації нових членів – насамперед серед молоді, – координації дій і фінансування через криптовалютні транзакції [18]. За даними J. Berger і J. Morgan, ІДІЛ у пік своєї активності публікувала до 90 тисяч повідомлень на добу в різних соціальних мережах [19]. Децентралізований і транснаціональний характер такої діяльності суттєво ускладнює її моніторинг та блокування.

Не менш небезпечним виміром інформаційних загроз є цілеспрямовані інформаційні операції та дезінформація. Поширення фейкових новин, маніпуляція громадською думкою та дестабілізація суспільства через скоординовані інформаційні кампанії стали ключовим елементом сучасної гібридної війни [10]. Збройна агресія Росії проти України супроводжується масштабними інформаційними атаками, спрямованими на підрив довіри до державних інституцій, провокування паніки та деморалізацію населення.

Нарешті, усі зазначені форми терористичної активності в онлайн-просторі спираються на використання анонімних мереж і зашифрованих комунікацій. Мережі Tor та I2P, а також зашифровані месенджери активно застосовуються терористами для конспіративного спілкування, уникнення ідентифікації та збуту заборонених товарів у середовищі Darknet [6]. Це принципово ускладнює роботу правоохоронних органів і спецслужб у режимі реального часу.

Транснаціональна природа описаних загроз робить неможливою ефективну протидію ним виключно засобами окремих держав, тому міжнародна координація є необхідною умовою успіху антитерористичних зусиль. На рівні ООН ключову координаційну роль відіграють Контртерористичний комітет (Counter-Terrorism Committee, CTC) та Управління ООН з питань боротьби з тероризмом (UN Office of Counter-Terrorism, UNOCT), які розробляють загальносистемні стратегії і стандарти протидії використанню ІКТ у терористичній діяльності [13]. Резолюція Ради Безпеки ООН 1373 (2001) заклала правову основу для міжнародного співробітництва у цій сфері. Було запроваджено Центр передового досвіду НАТО з питань кіберзахисту (CCDCOE) у Таллінні, який проводить дослідження у сфері кібербезпеки, розробляє Таллінське керівництво з міжнародного права стосовно кібернетичних операцій і формує спільні стандарти поведінки держав у кіберпросторі [5].

Важливу роль у системі міжнародної протидії відіграє й Європейський центр боротьби з кіберзлочинністю (EC3) у структурі Європолу, який координує розслідування злочинів і терористичних дій в онлайн-середовищі, здійснює аналіз загроз і підтримує оперативний обмін розвідувальними даними між державами – членами ЄС [20]. Зусилля міжурядових структур доповнюються діяльністю приватного сектору: Глобальний інтернет-форум з протидії тероризму (Global Internet Forum to Counter Terrorism, GIFCT), заснований у 2017 р. провідними технологічними компаніями (YouTube, Facebook, Microsoft і Твіттер), запровадив спільну базу хешів – своєрідний «відбиток» терористичного контенту – що дозволяє автоматично виявляти й видаляти пропагандистські матеріали з платформ. Використання алгоритмів штучного інтелекту та машинного навчання у цьому процесі дозволяє масштабувати протидію та скорочувати час реагування [3].

Поряд із міжнародними механізмами надзвичайно важливим є накопичений провідними державами національний досвід формування систем кіберзахисту. Сполучені Штати Америки мають найбільш розвинену систему кібербезпеки та протидії тероризму: Агентство національної безпеки (National Security Agency, NSA), Агентство з кібербезпеки та безпеки інфраструктури США (Cybersecurity and Infrastructure Security Agency, CISA) і Федеральне бюро розслідувань (Federal Bureau of Investigation, FBI) здійснюють скоординований моніторинг кіберпростору. «Патріотичний акт» (USA PATRIOT Act) надав розширені повноваження для відстеження електронних комунікацій, водночас спровокувавши тривалу суспільну дискусію щодо меж допустимого

державного втручання в приватне життя [6]. Ізраїль, у свою чергу, є визнаним світовим лідером у сфері кібербезпеки: підрозділ 8200 Сил оборони країни спеціалізується на кіберрозвідці та нейтралізації цифрових загроз, а ізраїльська практика активного моніторингу соціальних мереж і систем раннього виявлення радикалізації вважається одним із найефективніших підходів у світі й активно вивчається іншими державами [9].

Європейський Союз, у свою чергу, розробив комплексну нормативно-правову базу кібербезпеки: Директива NIS2 (2022/2555) встановлює мінімальні обов'язкові стандарти безпеки для операторів критичної інфраструктури, а Регламент (ЄС) 2021/784 зобов'язує цифрові платформи видаляти терористичний контент протягом однієї години після отримання відповідного повідомлення [20]. Така регуляторна архітектура забезпечує системність і юридичну визначеність у сфері протидії тероризму в цифровому середовищі. Особливого розгляду заслуговує досвід України, яка напрацювала унікальну практику протистояння кібератакам і гібридним загрозам, що має значення далеко за межами країни. Закон України «Про основні засади забезпечення кібербезпеки України» (2017) заклав правові основи захисту кіберпростору, а Стратегія кібербезпеки України (2021) визначила стратегічні пріоритети на середньострокову перспективу. Створення Центру протидії дезінформації при РНБО, розбудова спеціалізованих кіберпідрозділів у складі Збройних Сил і розвиток партнерства з міжнародними організаціями дозволили ефективно протистояти безпрецедентному тиску в інформаційному просторі.

Попри помітний прогрес, глобальна система інформаційної безпеки в антитерористичному контексті стикається з низкою суттєвих проблем. Передусім, стрімкий технологічний розвиток випереджає можливості правоохоронних органів адаптуватися до нових загроз: поява квантових обчислень, генеративного штучного інтелекту та deepfake-технологій відкриває терористам якісно нові інструменти маніпуляції та конспірації [11]. Тісно пов'язаною з цим є проблема балансу між безпекою та правами людини: розширений моніторинг інформаційного простору неминуче ставить питання дотримання права на приватність і свободу слова, формуючи поле постійних правових і суспільних колізій [6]. Окремим викликом залишається правова і юрисдикційна фрагментація: глобальний характер Інтернету та суттєві відмінності національних законодавств ускладнюють міжнародне переслідування кіберзлочинців і терористів, що діють на території різних держав [5]. Технологічний розрив між розвиненими державами та країнами, що розвиваються, залишається суттєвим: обмеженість ресурсів для створення ефективних систем кібербезпеки в останніх формує вразливі ланки у глобальній архітектурі інформаційної безпеки [1].

З урахуванням виявлених проблем та узагальнення міжнародного досвіду за результатами проведеного дослідження сформульовано комплекс практичних рекомендацій. Першочерговим напрямом є розвиток технологій штучного інтелекту для автоматичного виявлення терористичного контенту, аналізу великих масивів даних і прогнозування загроз на основі поведінкових патернів – впровадження таких систем дозволить суттєво підвищити швидкість реагування на нові загрози [4]. Поряд із цим необхідне посилення міжнародної правової бази через укладення конвенцій про кібербезпеку та протидію кібертероризму, гармонізацію відповідних національних законодавств з міжнародними стандартами і вироблення обов'язкових норм поведінки держав у кіберпросторі [13]. Практичне значення матиме і створення глобальної платформи обміну інформацією про кіберзагрози в режимі реального часу, що інтегрує дані від державних, міжурядових і приватних структур із використанням уніфікованих протоколів обміну даними. Водночас необхідні інвестиції в підготовку фахівців у сфері кібербезпеки та контртероризму, включно з програмами двосторонньої і багатосторонньої технічної допомоги країнам, що розвиваються, з метою подолання технологічного розриву [1]. Реалізація зазначених заходів потребує розбудови механізмів співпраці держав і приватного сектору, технологічних корпорацій, академічної спільноти і структур громадянського суспільства для спільного вироблення стандартів і реагування на загрози. Нарешті, ефективним доповненням технологічних і правових інструментів стане впровадження масштабних програм цифрової грамотності, спрямованих на підвищення стійкості населення до пропаганди та дезінформаційних операцій, а також розроблення систем раннього виявлення онлайн-радикалізації, заснованих на мережевому аналізі та моніторингу поведінкових індикаторів із суворим дотриманням міжнародних стандартів у сфері прав людини [8].

Висновки. Проведене дослідження дозволяє стверджувати, що інформаційна безпека стала невід'ємною та критично важливою складовою в міжнародно-правовому механізмі протидії теро-

ризму. Цифрова трансформація суспільства кардинально змінила природу терористичних загроз: сучасні терористичні організації активно використовують ІКТ для координації, пропаганди, вербування, фінансування та безпосереднього здійснення атак на критичну інфраструктуру держав.

Встановлено, що ефективна протидія інформаційним загрозам терористичного характеру вимагає комплексного, міждисциплінарного підходу, що органічно поєднує технологічні, правові, організаційні та міжнародні механізми. Жоден з цих компонентів сам по собі не є достатнім: лише їх системна взаємодія здатна забезпечити адекватну відповідь на багатовимірний характер сучасних загроз.

Міжнародна співпраця, оперативний обмін розвідувальними даними, розвиток передових технологій і партнерство з приватним сектором виступають ключовими факторами ефективності. Досвід України у протидії російській агресії та гібридним загрозам наочно демонструє важливість інтеграції інформаційної безпеки в загальну систему національної безпеки та переваги міжнародного партнерства в умовах асиметричного протистояння.

Водночас залишаються актуальними проблеми забезпечення балансу між потребами безпеки й захистом прав людини, гармонізації міжнародного законодавства та подолання технологічного розриву між державами. Перспективними напрямами подальших досліджень є розробка адаптивних правових стандартів поведінки у кіберпросторі, вдосконалення механізмів міжнародного партнерства та дослідження можливостей застосування технологій штучного інтелекту в системах раннього виявлення кіберзагроз.

Відтак, інформаційна безпека є не другорядним, а центральним елементом сучасної архітектури глобальної безпеки, без належного забезпечення якого ефективна протидія тероризму у XXI столітті є принципово неможливою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Global Cybersecurity Index. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Cybersecurity-Index.aspx.
2. Conway M. Terrorist «Use» of the Internet and Fighting Back. Information & Security. *An International Journal*. 2006. Vol. 19. P. 9–30.
3. Klausen J. Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. *Studies in Conflict & Terrorism*. 2015. Vol. 38. No. 1. P. 1–22. URL: https://www.tandfonline.com/doi/pdf/10.1080/1057610X.2014.974948.
4. Wilson C. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Washington: Congressional Research Service, 2005. 46 p. URL: https://www.everycrsreport.com/files/20050401_RL32114_1729f8812bf5a0b031dcb5b714921fe531634223.pdf.
5. Schmitt M.N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: Cambridge University Press, 2017. 569 p.
6. Etzioni A. Privacy in a Cyber Age: Policy and Practice. New York: Palgrave Macmillan, 2015. 248 p.
7. Hoffman B. Inside Terrorism. 3rd ed. New York: Columbia University Press, 2017. 528 p.
8. Denning D.E. Terror's Web: How the Internet is Transforming Terrorism. Handbook of Internet Crime / Y. Jewkes, M. Yar (eds.). Willan Publishing, 2009. URL: https://scispace.com/pdf/terrors-web-how-the-internet-is-transforming-terrorism-3pji2deqlf.pdf.
9. Weimann G. Terrorism in Cyberspace: The Next Generation. Washington, D.C. Woodrow Wilson Center Press. 2015. 296 p.
10. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux, 2020. 528 p.
11. Buchanan B. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge: Harvard University Press, 2020. URL: https://www.researchgate.net/publication/392622180_Ben_BUCHANAN_The_Hacker_and_the_State_Cyber_Attacks_and_the_New_Normal_of_Geopolitics_Cambridge_Harvard_University_Press_2020.
12. Довгань О.Д., Ткачук Т.Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. URL: https://ippi.org.ua/dovgan-od-tkachuk-tyu-pravove-zabezpechennya-informatsiinoi-bezpeki-derzhavi-yak-pidgaluz-informatsi.

13. United Nations Security Council. Resolution 2341 (2017) on Protection of Critical Infrastructure against Terrorist Attacks. UN Doc. S/RES/2341, 13 February 2017. URL: https://docs.un.org/en/s/res/2341(2017).
14. Von Solms R., Van Niekerk J. From Information Security to Cyber Security. *Computers & Security*. 2013. Vol. 12. No.1. P. 97–102.
15. Whitman M.E., Mattord H.J. Principles of Information Security. 6th ed. Boston: Cengage Learning, 2018. 711 p. URL: https://unidel.edu.ng/focelibrary/books/Principles%20of%20Information%20Security%20by%20Whitman,%20Michael%20Mattord,%20Herbert%20(z-lib.org).pdf.
16. Jarvis L., Macdonald S., Nouri L. The Cyberterrorism Threat: Findings from a Survey of Researchers. *Studies in Conflict & Terrorism*. 2014. Vol. 37. No. 1. P. 68–90.
17. Greenberg A. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Doubleday, 2019. 368 p.
18. Hsinchun C. Dark Web: Exploring and Data Mining the Dark Side of the Web. URL: http://repo.darmajaya.ac.id/4446/1/Dark%20Web_%20Exploring%20and%20Data%20Mining%20the%20Dark%20Side%20of%20the%20Web%20%28%20PDFDrive%20%29.pdf.
19. Berger J. M., Morgan J. The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter. URL: https://www.brookings.edu/articles/the-isis-twitter-census-defining-and-describing-the-population-of-isis-supporters-on-twitter.
20. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023. The Hague: Europol, 2023. URL: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023.

Дата першого надходження рукопису до видання: 25.01.2026
Дата прийняття до друку рукопису після рецензування: 20.02.2026
Дата публікації: 5.03.2026