РОЗДІЛ 11
МІЖНАРОДНЕ ПРАВО

УДК 351/327.5
DOI https://doi.org/10.24144/2307-3322.2021.65.64

ПОЛІТИКА МІЖНАРОДНИХ ОРГАНІЗАЦІЙ З ПИТАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кононенко В.П.
доктор юридичних наук, доцент кафедри міжнародних відносин, міжнародної інформації та безпеки Харківського національного університету імені В. Н. Каразіна
https://orcid.org/0000-0002-6461-7072

Новікова Л.В.
кандидат юридичних наук, доцент завдувач кафедри міжнародних відносин, міжнародної інформації та безпеки Харківського національного університету імені В. Н. Каразіна
https://orcid.org/0000-0002-4640-2908

Копицька П.О.
студент Харківського національного університету імені В. Н. Каразіна

Кононенко В.П., Новікова Л.В., Копицька П.О. Політика міжнародних організацій з питань інформаційної безпеки

Статтю присвячено вивченню проблеми міжнародної інформаційної безпеки, яка є частиною загальної міжнародної безпеки і визначається як стан міжнародних відносин, що виключає порушення світової стабільності і створення загрози безпеці держав і світової спільноти в інформаційному просторі.

Інформаційні загрози є новим викликом міжнародному миру та безпеці, а тому для ефективної протидії міжнародному співтовариству необхідно адаптуватись к сучасним реаліям. Оскільки міжнародні організації створюються для об'єднання зусиль держав у досягненні певних цілей, вони (організації) також повинні адаптуватись трансформуючи свою політику в галузі міжнародної безпеки і, зокрема, у сфері безпеки інформаційної. Відповідно, предметом дослідження є трансформація політики міжнародних організацій у сфері інформаційної безпеки.

Адаптація міжнародних організацій до нових загроз відбувається за двома напрямками:

1) трансформація структури самої міжнародної організації;
2) трансформація політики безпеки міжнародних організацій.

Трансформацію політики безпеки міжнародних організацій можна поділити на внутрішню та зовнішню.

Внутрішня трансформація політики безпеки міжнародних організацій передбачає переорієнтацію (або доповнення) їх цілей діяльності. Якщо раніше, кажучи про глобальну безпеку, малася на увазі лише військово-політична безпека, то сьогодні – це також і продовольча безпека, і кліматична безпека, космічна, енергетична і інформаційна безпека.

Зовнішня трансформація політики безпеки міжнародних організацій передбачає тісну співпрацю з регіональними організаціями, відомствами та урядами держав (відповідно до рівня комунікації) у сфері інформаційної безпеки.

Захищаючи свої інформаційні інтереси, кожна держава має дбати про інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України повинна формуватися як складова її національної безпеки та частина соціально-економічної політики, виходячи з пріоритетності національних інтересів та загроз. Із правової точки зору вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством

Ключові слова: міжнародна інформаційна безпека, міжнародні організації, кібербезпека

Kononenko V.P., Novikova L.V., Kopytska P.O. Policy of international organizations on information security

The article is devoted to the study of the problem of international information security. It is part of overall international security. International information security is a state of international relations that excludes a violation of global stability and threats to the security of states in the information space.

Information threats are a new challenge to international peace and security. Therefore, for effective counteraction, it is necessary to adapt to modern realities. Since international organizations are created to unite the efforts of states to achieve certain goals, they (organizations) must also adapt to changes. They must transform their policy in the field of international security and, in particular, in the field of information security. Accordingly, the subject of this research is the transformation of the policy of international organizations in the field of information security.

International organizations are adapting to new threats in two directions:

1) transformation of the structure of the international organization itself;

2) transformation of the security policy of international organizations.

The transformation of the security policy of international organizations can be divided into internal and external.

The internal transformation of the security policy of international organizations presupposes a reorientation (or additions) of their goals of activity. If earlier, speaking of global security, they meant only military-political security, today it is also food security, climate security, space, energy and information security.

External transformation of the security policy of international organizations presupposes close cooperation with regional organizations, departments and governments of states (according to the level of communication) in the field of information security.

Defending its information interests, each state must take care of information security. The strengthening of the Ukrainian statehood also requires the same. A balanced state information policy of Ukraine should be formed as an integral part of its national security. And also as a part of socio-economic policy in accordance with the priorities of national interests and threats. From a legal point of view, it is based on the principles of a rule-of-law democratic state and is implemented through the development and implementation of relevant national doctrines, strategies, concepts and programs in accordance with applicable law.

Keywords: international information security, international organizations, cyber security

Постановка проблеми. Світ стрімко змінюється і його сталий розвиток вже немислимий без цілеспрямованої глобальної інформатизації, з одного боку, і підвищення ступеня уразливості військових, технічних, енергетичних, соціальних об'єктів від інформаційного впливу – з іншого. Міжнародне співробітництво у сфері інформаційної безпеки зумовлює необхідність пошуку спільних рішень, організацій засобів протидії інформаційним та кіберзагрозам, вироблення спільної стратегії інформаційної безпеки для протидії інформаційному тероризму та злочинності. Для досягнення зазначених цілей міжнародним організаціям необхідно трансформувати свою політику у сфері інформаційної безпеки.

Розвиток ефективних інструментів забезпечення інформаційного суверенітету є важливою умовою суспільного розвитку і першочерговим завданням сьогодення. Питання забезпечення інформаційної безпеки є надзвичайно важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу.

Стан опрацювання цієї проблематики. Загальні питання безпеки висвітлювали в своїх працях В. Ф. Антипенко, О.В. Бєглий, І.І. Лукашук, А.В. Назаренко, Л.Д. Тимченко та ін. Міжнародно-правові проблеми забезпечення глобальної безпеки на сучасному етапі вивчала Н.М. Ємельянова. Захисту національних інтересів України в сфері кіберпростору присвятили свої праці Д.В. Дубов та М.А. Ожеван. Питання інформаційної безпеки України щодо сучасних викликів, загроз та механізмів протидії негативним інформаційно-психологічним впливам вивчала У. Ільницька.

Міжнародний і зарубіжний досвід забезпечення інформаційної безпеки як складової системи національної безпеки вивчав А.В. Войціховський.

Правові засади інформаційної безпеки України та питання її правового регулювання вивчали П.Д. Біленчук та А.Ю. Нашинець-Наумова. Конституційно-правові засади національної безпеки України розглядав В.О. Антонов. О.Д. Довгань та І.М. Доронін відслідковують ескалацію кіберзагроз національним інтересам України та вивчають правові аспекти кіберзахисту. К.Ю. Ісмайлов аналізував співвідношення понять «кібербезпека та «інформаційна безпека». О.М. Фролова розглядала роль ООН в системі міжнародної інфор-

маційної безпеки. Питання трансформація політики міжнародних організацій у сфері інформаційної безпеки цілеспрямовано не досліджувалось, що вимагає більш уважного ставлення до даної тематики.

Метою статті є дослідження особливостей забезпечення міжнародної інформаційної безпеки державами, і, зокрема, трансформації політики міжнародних організацій у сфері інформаційної безпеки у зв'язку з новими викликами сучасності.

Виклад основного матеріалу. Хоча ключову роль в сучасній системі міжнародних відносин продовжують грати незалежні національні держави, дедалі активнішу участь у системі міжнародних відносин стали приймати нові актори – міжнародні організації (далі – МО) [1]. В процесі своєї діяльності міжнародна організація набуває власних, відмінних від початково зафіксованих в установчому договорі, прав та обов'язків, реалізуючи повноваження прямо не визначені, але зумовлені її цілями [2, с. 314-315]. Це тим більш важливо, що МО створюються для об'єднання зусиль держав у досягненні певних завдань [3, с. 227]. Але, оскільки міжнародне життя не є сталою категорією, зазначені цілі можуть змінюватись, що потребує відповідної трансформації і політики міжнародних організацій. МО, які не адаптуються до викликів сьогодення, втрачають свій авторитет і, навпаки, організації, що змінюють свою діяльність щоб відповідати новітнім вимогам, набувають більшого впливу. Як наслідок, зростання впливу таких суб'єктів світової політики – міжурядових і неурядових організацій формує нову ситуацію на міжнародній арені [4]. Саме вони виявляються досить ефективними майданчиками вирішення актуальних проблем сучасності та дають можливість державам брати участь в цьому за допомогою своїх структур [5, с. 24].

На думку Н.М. Ємельянової, усі виклики і загрози глибоко взаємопов'язані і стають все складнішими з кожним днем. Для зменшення зростаючих викликів безпеки світовій спільноті будуть потрібні зовсім нові форми взаємодії, засновані на міжнародному праві. У новому XXI ст. надійна безпека може бути тільки загальною і всеосяжною, вона повинна охопити всі держави і регіони, а також враховувати всі фактори, що впливають на міжнародну систему [6].

Останнім часом значно зростає інтенсивність споживання інформації в усіх сферах життєдіяльності людини і суспільства – соціальній, науково-технічній, технологічній, статистичній, економічній та ін. Процеси збору, накопичення, переробки та розповсюдження інформації стають необхідною умовою існуючих структур освіти, медицини, оборони, управління; здійснення ефективних політичних впливів, вирішення масштабних економічних задач. Однак інформація володіє і дестабілізуючим потенціалом для суспільства через її практично необмежені можливості впливу на людину і суспільство [7, с. 6].

Порівняно недавно з'явилися терміни «кібербезпека» і «інформаційна безпека», які на сьогоднішній день визначаються не зовсім коректно. Складність формулювання поняття «інформаційна безпека» полягає в тому, що сам предмет, безпека якого визначається, не окреслений як за внутрішньою структурою, так і за внутрішнім властивостям, які необхідні для формування вимог до його безпеки. На думку К.Ю. Ісмайлова, термін «інформаційна безпека» на даний момент часу не є коректним по своїй суті. Замість нього він пропонує вживати термін «інформаційна захищеність» і використовувати для нього таке визначення: інформаційна захищеність – це захист конфіденційності, цілісності та доступності інформації [8, с. 32-33]. Д.В. Дубов, М.А. Ожеван М.А. ототожнюють кібербезпеку з інформаційною безпекою [9, с. 4].

Захищаючи свої інформаційні інтереси, кожна держава має дбати про інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України повинна формуватися як складова її національної безпеки та частина соціально-економічної політики, виходячи з пріоритетності національних інтересів та загроз. Із правової точки зору вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством [10, с. 68]. Кожна держава або група держав виробляє власну стратегію поведінки та політики інформаційної безпеки в умовах сучасного розвитку комунікацій. Для європейської стратегії характерні пошуки рівноваги між контролем держави та стихією ринку, динамічним поєднанням державних інтересів і прагнень приватного та корпоративного бізнесу [11, с. 20-21]. Зважаючи на стрімкий розвиток інформаційно-комунікаційних технологій, тотальну комп'ютеризацію, створення глобального інформаційного простору з'явились принципово нові категорії – інформаційне суспільство, кіберпростір, що мають безмежний потенціал і значний вплив на політичний, економічний, соціальний і культурний розвиток держави. Саме створення інформаційного суспільства призвело до виникнення багатьох новітніх загроз у важливих сферах життєдіяльності суспільства (банківська, воєнна, критична інфраструктура тощо), тому інформаційну безпеку цілком виправдано розглядають як самостійний елемент національної безпеки [12, с. 284].

Інформаційна безпека, як поняття в міжнародних відносинах залежно від його використання розглядається у декількох ракурсах. У найзагальнішому вигляді– це стан захищеності інформаційного середовища

суспільства, який забезпечує його формування, використання і розвиток в інтересах особи, суспільства, держави. Інформаційна безпека включає в себе сукупність організаційних, соціально-економічних, юридичних заходів, спрямованих на забезпечення сталого розвитку суспільства і держави [13, с. 64]. Безпека в інформаційній сфері, на думку П.Д. Біленчука, передбачає забезпечення інформаційного суверенітету; удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження сучасних технологій у цій сфері, наповнення інформаційного простору достовірною інформацією; забезпечення конституційного права громадян на свободу слова, доступу до інформації, недопущення протиправного втручання органів державної влади у діяльність засобів масової інформації; вживання комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери держави [13, с. 54-55]. Про інформаційний суверенітет також пише і О.Р. Вайцеховська [14, с. 243].

Осмислення сукупності інформаційних процесів щодо забезпечення їх безпеки має велике значення як для окремого суспільства, так і міжнародного співтовариства в цілому. Якісно новий підхід, який би розглядав інформаційну безпеку не тільки в конкретно-прикладних аспектах, а як внутрішній стан всієї соціальної системи, представляється перспективним напрямком у вивченні проблем даної галузі, що забезпечує ефективне функціонування та успішний розвиток як інформаційної сфери, так і соціуму в цілому [15, с. 3-4].

Важливу участь у безпекових заходах традиційно бере ООН. Її діяльність у сфері інформаційної безпеки спрямована на розробку міжнародно–правової бази та вироблення документів для протидії протиправному використанню науково-технологічного прогресу терористичними угрупованнями та організованою злочинністю. Проблема інформаційної безпеки в контексті формування глобального інформаційного суспільства стала актуальною для діяльності спеціалізованих установ ООН, зокрема, ЮНЕСКО та МСЕ, враховуючи гуманітарні та технічні програми та проекти організацій [16].

Модернізація політики інформаційної безпеки на рівні ООН зумовлена появою нових чинників відповідальної поведінки держав, приватного сектора, доктрини і організацій громадянського суспільства у кіберпросторі, яка могла б сприяти підвищенню ефективності міжнародної протидії новим викликам. Питання міжнародної інформаційної безпеки упродовж 1998-2015 рр. постійно обговорювалось на Генеральній Асамблеї ООН з метою розробки відповідного міжнародного документа на основі резолюцій «Роль науки і техніки в контексті міжнародної безпеки і роззброєння» та «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки», в яких містилися положення про використання високих технологій у цивільній і у воєнній сферах, про застосування досягнень науки і техніки у модернізації сучасних озброєнь, про важливість протидії деструктивним впливам [17, с. 103]. Міжнародна інформаційна безпека визначається ООН як стан міжнародних відносин, що виключає порушення світової стабільності і створення загрози безпеці держав і світової спільноти в інформаційному просторі [18, с. 61]. Враховуючи поширення кіберзагроз Генеральна Асамблея ООН у 2019 р. ухвалила резолюцію під назвою «Заохочення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки», в якій підтверджується необхідність створення відкритого, безпечного, стабільного, доступного і мирного інформаційно – комунікаційного середовища, встановлення довірчих відносин між державами, розширення можливостей держав щодо співпраці і заохочення використання новітніх технологій, що сприятимуть зменшенню ризику виникнення конфліктів, і яка є суттєво важливою для забезпечення міжнародної безпеки [19, с. 103-104]. Також, в ООН створено Групу високого рівня з питань загроз, викликів і змін, розглядаються питання про створення єдиного координатора ООН по боротьбі з тероризмом, комісії із світобудівництва.

На рівні Європи до останнього часу проблема кібербезпеки була вирішена лише частково – у сфері протидії кіберзлочинності. Йдеться про прийняту Радою Європи у 2001 р. Конвенцію про кіберзлочинність, що відносила до сфери кіберзлочинів такі. 1. Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ до комп'ютерної системи або її частини; нелегальне перехоплення комп'ютерних даних; втручання в комп'ютерні дані; втручання у комп'ютерну систему; зловживання пристроями. 2. Правопорушення, пов'язані з комп'ютерами: підробка, пов'язана з комп'ютерами; шахрайство, пов'язане з комп'ютерами. 3. Правопорушення, пов'язані зі змістом: правопорушення, пов'язані з дитячою порнографією. 4. Правопорушення, пов'язані з порушенням авторських та суміжних прав. Невизначеність на глобальному рівні та відсутність єдиних підходів змушує керівництво держав формувати політику кібербезпеки на національному рівні. Більшість держав світу вже створили відповідні підрозділи (як правоохоронні, так і військові), призначені для протидії кіберзагрозам та розроблення наступальних технологій [9, с. 3-4]. У зв'язку з розумінням важливості проблеми кібербезпеки в Європейському Союзі у 2004 р. було створено Європейське агентство з мережевої та інформаційної безпеки. У 2012 р. це Агентство оприлюднило огляд «Національні стратегії кібербезпеки. Практичний посібник з розвитку та виконання».

Щодо визначення терміну «кібербезпека» в цьому огляді констатовано факт, що в національних стратегіях не існує загальноприйнятого та однозначного визначення кібербезпеки [20, с. 16]. Усвідомлюючи той факт, що ефективність забезпечення інформаційної безпеки в європейському кіберпросторі також залежить від розвитку співпраці держав у рамках міжнародних органів у 2013 р. в структурі Європейського поліцейського офісу (Європол) був утворений Європейський центр боротьби з кіберзлочинністю. Розуміючи актуальність проблеми забезпечення інформаційної безпеки як складової системи національної безпеки, більшість держав світу почали здійснювати внутрішньодержавні комплексні заходи з безпеки в кіберпросторі. Ці заходи пов'язані, перш за все, з розробкою і вдосконаленням національного законодавства в даній галузі і створенням спеціалізованих структур, що відповідають за безпеку в кіберпросторі [12, с. 285].

Серед міжнародних організацій, основною метою яких є саме безпека, НАТО найбільш ефективно модернізувала політику щодо інформаційної безпеки. Організація заснувала центри у країнах-членах як багатонаціональні інститути для розробки доктрини кібербезпеки, вдосконалення міждержавної взаємодії, впровадження теоретичних напрацювань у практиці протидії кіберзагрозам, обміну досвідом кіберзахисту представників країн-членів і країн-партнерів. Наразі Центр кібербезпеки НАТО функціонує в Естонії, він не є підрозділом військового командування або структури збройних сил НАТО, а персонал та фінансування забезпечуються державами-спонсорами та державами-учасниками [19].

Важливу роль у зміцненні кібербезпеки, безпеки інформаційно-комунікаційних технологій відіграє ОБСЄ, працюючи над зниженням ризиків виникнення конфліктів між державами в результаті використання інформаційних технологій. Ключовою проблемою в цьому відношенні є практична реалізація відповідних директив ООН групами урядових експертів на регіональному рівні. Для розробки сумісного підходу ОБСЄ до проблем кібербезпеки та визначення завдань ОБСЄ, у Відні 9-10 травня 2011 р. було проведено конференцію «Загальний підхід до кібербезпеки: визначення майбутньої ролі ОБСЄ». У 2013 р. ОБСЄ прийняла інноваційні рекомендації про заходи щодо зміцнення довіри у сфері кібербезпеки, спрямовані на підвищення прозорості та забезпечення безпеки в регіоні, які передбачали взаємодію з приватними компаніями і провайдерами найважливішої інфраструктури, а також спільні підходи до управління кібербезпекою [21].

Відповідно, Україна повинна продовжувати адаптацію свого законодавства [див.: 22] до нормативних актів ЄС, але, також, і враховуючи новітні напрацювання міжнародних організацій, розвиток міжнародного права з розглядуваного питання та практику міжнародних судових установ [23, с. 95].

Висновки. Адаптація міжнародних організацій до нових загроз відбувається за двома напрямками:

1) трансформація структури самої міжнародної організації. Наприклад, в ООН створено Групу високого рівня з питань загроз, викликів і змін, розглядаються питання про створення єдиного координатора ООН по боротьбі з тероризмом, комісії із світобудівництва тощо;
2) трансформація політики безпеки міжнародних організацій.
2. Трансформацію політики безпеки міжнародних організацій можна поділити на внутрішню та зовнішню.
3. Внутрішня трансформація політики безпеки міжнародних організацій передбачає переорієнтацію (або доповнення) їх цілей діяльності. Якщо раніше, кажучи про глобальну безпеку, мали на увазі лише військово-політичну безпеку, то сьогодні – це також і продовольча безпека, і кліматична безпека, космічна, енергетична і інформаційна безпека.
4. Зовнішня трансформація політики безпеки міжнародних організацій передбачає тісну співпрацю з регіональними організаціями, відомствами та урядами держав (відповідно до рівня комунікації) у сфері інформаційної безпеки.

Список використаних джерел:

1. Снапковский В.Е. Международные организации в системе международных отношений. *Белорусский журнал международного права и международных отношений*. 2000. № 3. URL: http://evolutio.info/ru/journal-menu/2000-3/2000-3-snapkovski (дата звернення: 01.07.2021).

2. Міжнародне публічне право: підручник: у 3 т. за заг. ред. В. Ф. Антипенка. К. : НАУ, 2012. Т. 1. 420 с.

3. Кононенко В.П., Тимченко Л.Д. Міжнародне право: підручник. К.: Знання, 2012. 631 с.

4. Мисту Г.М. Международные организации как участники мировой политики и международных отношений : дис. ... канд. полит. наук : М., 2006 212 с. URL: https://www.dissercat.com/content/mezhdunarodnye-organizatsii-kak-uchastniki-mirovoi-politiki-i-mezhdunarodnykh-otnoshenii (дата звернення: 11.05.2021).

5. Батур А.Г.А. Мохаммад. Роль международных организаций в урегулировании афганского конфликта в XXI веке: дисс. … канд. полит. наук. Санкт-Петербург, 2017. 358 с.

6. Емельянова Н.Н. Международно-правовые проблемы обеспечения глобальной безопасности на современном этапе: дисс. ... докт. юрид. наук. Москва, 2013.404 с. URL: https://www.dissercat.com/content/mezhdunarodno-pravovye-problemy-obespecheniya-globalnoi-bezopasnosti-na-sovremennom-etape-0 (дата звернення: 11.05.2021).

7. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ:«Гельветика», 2017.168 с.

8. Ісмайлов К.Ю. Поняття «кібезбезпека та «інформаційна безпека». Типологія безпеки. Міжнародна науково-практична конференція «Актуальні проблеми автоматизації та управління». Луцьк, 2016. С. 32-33.

9. Дубов Д.В., Ожеван М.А. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців: аналітична доповідь. НІСД. 2012. 28 с.

10. Бондар І.Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014, № 1. С. 68-75.

11. Парахонський Б.О. Зовнішня політика України в умовах кризи міжнародного безпекового середовища: аналіт. доп. К.: НІСД, 2015. 100 с.

12. Войціховський А.В. нформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). Вісник Харківського національного університету імені В.Н.Каразіна. Серія«ПРАВО». 2020. № 29. С. 281-288.

13. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.

14. Вайцеховська О.Р. Міжнародний фінансовий правопорядок: теоретичні засади та актуальні проблеми в умовах глобалізації. Дис. … докт. юрид. наук. Харків, 2020. 472 с.

15. Манжуева, О.М. Феномен информационной безопасности: сущность и особенности : автореф. дис. … д-ра филос. Наук. Улан-Удэ, 2015. 25 с.

16. Фролова О.М. Роль ООН в системі міжнародної інформаційної безпеки. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140 (дата звернення 20.06.2021).

17. Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. Політичне життя. 2020. № 1. С. 102-109.

18. Болгов Р.В. Деятельность ООН в области информации и международные аспекты информационной безопасности России. Сравнительная политика. 2019. №1. С. 59-69.

19. NATO Cooperative Cyber Defence Centre (CCDCOE). URL: https://www.cybersecurityintelligence.com/ nato-cooperative-cyber-defence-centre-ccdcoe-395.html (дата звернення 20.06.2021).

20. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. К.: Видавничий дім «АртЕк». 2017. 107 с.

21. Organization for Security and Co-operation in Europe – OSCE. URL: https://www.osce.org/whatistheosce (дата звернення 20.06.2021).

22. Кононенко В.П. Законодавство чи закон? *Право України*. 2004. № 4. С. 96-98.

23. Кононенко В.П. Вирішення територіальних спорів Міжнародним Судом ООН: теорія і практика: монографія. Київ-Одеса: «Фенікс», 2018. 438 с.