Bulletin of Taras Shevchenko National University of Kyiv.
Legal Studies, 2023; 1(125): 21-26
УДК 314
DOI: https://doi.org/10.17721/1728-2195/2023/1.125-4

ISSN 1728-2195

І. Брацук, канд. юрид. наук, доц.
ORCID ID: 0000-0003-0164-7407,
С. Кавин, асп.
ORCID ID: 0000-0002-6189-3848
Львівський національний університет імені Івана Франка, Львів, Україна

МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В РАМКАХ ООН

Стаття присвячена аналізу та вивченню правових механізмів ООН у сфері забезпечення інформаційної безпеки. Проаналізовано особливості функціонування інституційно-правового механізму інформаційного захисту в рамках координації ООН у контексті багатовекторної системи міжнародної безпеки та правового регулювання міжнародного співробітництва. Обґрунтовано доцільність розробки інтегрованої, скоординованої інформаційної політики міжнародних організацій та інституцій з метою уніфікації підходів до забезпечення інформаційної безпеки. Проведено узагальнення основних проблем, що виникають у міжнародному правовому регулюванні боротьби у сфері забезпечення інформаційної безпеки й основних загроз міжнародному миру в інформаційному просторі та запропоновано шляхи їхньої вирішення. Узагальнено принципи міжнародної інформаційної безпеки, виокремлено основні тенденції розвитку кіберзагроз у сучасному інформаційному просторі та заходи, необхідні для їх нейтралізації. Аналізуються особливості функціонування інституційно-правового механізму кіберзахисту в контексті законодавчої регламентації міжнародного співробітництва між міжнародними організаціями та інституціями. Зокрема, проведено аналіз основних механізмів правового забезпечення кіберзахисту інформаційного простору з метою їхньої інтеграції в єдину міжнародну систему правового інформаційного поля.

Ключові слова: міжнародна інформаційна безпека; міжнародне право; міжнародні організації; ООН; міжнародно-правові акти; резолюція; правові механізми; конвенції.

Вступ

Актуальність проблематики: Міжнародні правові акти щодо міжнародної інформаційної безпеки, які приймаються у форматі міжнародних організацій, зокрема ООН, виступають керівними принципами діяльності багатосторонніх міжнародних відносин із врахуванням позицій та інтересів усіх міжнародних учасників, як інституцій, так і держав. Проблема інформаційної безпеки в контексті формування глобального інформаційного суспільства стала актуальною для діяльності спеціалізованих установ ООН, зокрема ЮНЕСКО та МСЕ. Відповідно комплексне дослідження загальних закономірностей функціонування та розвитку міжнародно-правових механізмів забезпечення інформаційної безпеки в рамках ООН є особливо доречним, актуальним

Постановка проблеми. У результаті активного впровадження цифрових технологій у всі сфери життя суспільства на передній план виходять як міжнародні, так і національні правові механізми, які спрямовані на забезпечення дотримання безпеки інформаційного простору. Ці правові механізми передбачають удосконалення й гармонізацію нормативно-правової бази у сфері інформаційної безпеки як на національному, так і міжнародному рівнях. Проте оскільки останніми роками активно просувається ідея цифрового суверенітету, це у свою чергу зумовлює необхідність дослідження комплексу питань, які пов'язані із забезпеченням і дотриманням контролю над інформацією, комунікацією, даними та інфраструктурою, пов'язаною з інтернетом. Це, у свою чергу, зумовлює необхідність вивчення правових механізмів завдяки яким забезпечується захист інформаційної безпеки. Таким чином, дослідження цієї проблематики саме в рамках ООН є особливо доцільним, актуальним та потребує детального аналізу.

Мета дослідження: комплексне вивчення загальних закономірностей функціонування та розвитку міжнародно-правових механізмів забезпечення інформаційної безпеки в рамках ООН і розробка науково-обґрунтованих пропозицій і рекомендацій стосовно ефективної дії даних механізмів у міжнародному й національних правопорядках.

Об'єкт дослідження: міжнародно-правові механізми забезпечення інформаційної безпеки в рамках ООН.

Предмет дослідження: міжнародні правові акти у сфері інформаційної безпеки.

Методологія: методологічну основу наукової роботи становлять загальнонаукові та спеціально-юридичні методи. Зокрема, у процесі дослідження використано системний підхід, метод узагальнення й системний аналіз.

Стан дослідження: на сучасному етапі розвитку інформаційного суспільства, інформаційна безпека ототожнюється із захистом. Зокрема, у розвідках Ф. Альхудхайр (F. Alkhudhayr), С. Альфаррадж (S. Alfarraj), Б. Альджамілі (B. Aljameeli), С. Елхдірі (S. Elkhdiri) *інформаційна безпека визначається як захист інформації, системи й апаратного забезпечення, які використовують, зберігають і передають повідомлення, для забезпечення цілісності, конфіденційності й доступності даних, а також захисту операційних процедур* [29, с. 1–6]. У наукових дослідженнях Н. Р. Мукундан (N. R. Mukundan), Л. Пракаш Сай (Sai L. Prakash) *інформаційна безпека визначається як збереження конфіденційності, цілісності та доступності інформації; а також інших її властивостей, таких, як автентичність, підзвітність, невідмовність* [38, с. 1].

У цьому контексті цікавим є визначення інформаційної безпеки в роботі польського дослідника-правознавця П. Потейко (P. Potejko). Він визначає інформаційну безпеку *як сукупність дій, методів і процедур, здійснюваних уповноваженими особами і спрямованих на забезпечення цілісності збирання, зберігання й обробки інформаційних ресурсів шляхом їхнього захисту від небажаного, несанкціонованого поширення, модифікації або знищення* [33, с. 194].

Проблемам інформаційної безпеки присвятили свої праці такі відомі зарубіжні фахівці, як М. К. Лібіцкі (M. C. Libicki) [29], Дж. С. Най (Nye J. S.) [30], А. Цебровскі (A. Cebrovski), Й. Гарстка (J. Garstka) [25],

Л. Брент (L. Brent) [24], Б. Дункан Холліс (Duncan B. Hollis) [26], С. Метью Ваксман (Matthew C. Waxman) [31], Кубо Мачак (Kubo Mačák) [28], Абід А. Адоніс (Abid A. Adonis) [22]. На основі їхніх досліджень були розроблені теорії інформаційних війн нового покоління та практики використання інформаційних озброєнь у міжнародних конфліктах. Акцент у роботах було сконцентровано на аналізі правового інструментарію інформаційних і кіберзагроз для системи міжнародної безпеки. Особливу увагу було приділено міжнародному нормативно-правовому співробітництву щодо інформаційної безпеки на рівні міжнародних організацій і провідних держав світу. Зокрема, було з'ясовано інституційні засади міжнародної інформаційної безпеки. Значний внесок у дослідження інформаційної безпеки в міжнародному вимірі зробили вітчизняні науковці, а саме О. Кучмій [3], Є. Макаренко [3], М. Рижков [3], О. Фролова [3], Г. Почепцов, М. Ожеван [3–4]. У своїх розвідках вони розвинули теоретичні положення стосовно проблеми міжнародної взаємодії у сфері інформаційної безпеки, особлива увага приділялась аналізу правової діяльності міжнародних інституцій у контексті характеристики міжнародних правових механізмів протидії новим викликам для системи міжнародної безпеки. У цьому контексті очевидною є необхідність вивчення інформаційної безпеки міжнародних організацій, а також практичного розглядання нових документів і рішень щодо їх інституційного забезпечення та імплементації у діяльності держав-учасниць.

Виклад основного матеріалу. Однією із перших зустрічей на міжнародному рівні з питань розвитку інформаційного суспільства й гарантування безпеки стала конференція "Інформаційне суспільство та розвиток", що відбулася в Мідранді (ПАР) 13–15 травня 1996 року ("Information Society and Development Conference" 13–15 May 1996 Gallagher Estate Miranda, South Africa). А вже 30 липня 1996 р. у Парижі відбулася нарада на рівні міністрів закордонних справ і міністрів із проблем тероризму. На цих засіданнях було акцентовано на важливості питання щодо небезпеки, пов'язаної з використанням терористами мереж і систем передавання інформації з метою злочинної діяльності, а відповідно – необхідності застосування засобів для запобігання таким діям [2].

За результатами конференції в Мідранді й наради в Парижі в 1998 р. на 53-й сесії Генеральної Асамблеї ООН було прийнято Резолюцію A/RES/53/70 [8], в якій уперше на найвищому рівні наголошувалося, що нові технології та засоби потенційно можуть бути використані в цілях, несумісних із задачами гарантування міжнародної стабільності й безпеки, та можуть негативно впливати на безпеку держав. Зауважимо, що Резолюція A/RES/53/70 поклала початок широкого обговорення питань міжнародної інформаційної безпеки та пошуку стратегій убезпечення суб'єктів міжнародних відносин від нових загроз.

У цьому контексті зазначимо, що відповідно до рекомендацій Резолюції A/RES/53/70, Інститутом ООН із проблем роззброєння (ЮНІДІР/UNIDIR/) і Департаментом з питань роззброєння Секретаріату ООН був організований міжнародний семінар з питань міжнародної інформаційної безпеки, який відбувся 1999 р. у Женеві. Завданням семінару було виявити підходи різних країн стосовно проблеми забезпечення інформаційної безпеки, оскільки кожна держава мала своє розуміння та бачення вирішення цієї проблеми.

Відповідно за робочими результатами дискусій семінару в 1999 р. на 54-й сесії ГА ООН було прийнято Резолюцію A/RES/54/50 [9], в якій визнаються можливості застосування досягнень науки і техніки як негативного чинника впливу на міжнародну безпеку.

На 55-й сесії ГА ООН було прийнято оновлену Резолюцію A/RES/55/28 (2000) [10], яка вперше вказала на загрози міжнародній інформаційній безпеці стосовно не тільки цивільної, а й військової сфер. За результатами роботи сесії було опубліковано Доповідь Генерального секретаря ООН (A/55/140/Corr. 1) [5]. У доповіді було сформовано основні принципи міжнародної інформаційної безпеки, які визначили норми поведінки держав в інформаційному просторі, а також заклали основу для міжнародних переговорів, зокрема під егідою ООН та інших міжнародних організацій із проблем міжнародної інформаційної безпеки. Також визначили роль ООН у контексті загальних зусиль цієї сфери. Уперше було наведено визначення понятійного апарату системи міжнародної інформаційної безпеки, а саме інформаційний простір, інформаційний ресурс, інформаційна війна, інформаційна зброя, інформаційна безпека.

Відповідно до рекомендацій Резолюції A/RES/55/28 (2000), на 55-й сесії ГА ООН було опубліковано доповідь Генерального секретаря ООН (A/56/164/Add.1) [6], в якій було виділено й описано основні чинники, які є найбільшими загрозами міжнародної інформаційної безпеки, а саме: розробка та використання засобів несанкціонованого втручання в роботу ІКТ, цілеспрямована інформаційна дія на критичні інфраструктури іншої держави; інформаційний вплив з метою підриву політичної, економічної та соціальної системи інших держав; ведення інформаційних війн тощо.

Згідно з Резолюцією ГА ООН A/RES/56/19 (2001) [11] було схвалено ідею створення (Групи високого рівня з питань загроз, викликів і змін) Групи урядових експертів держав – учасниць ООН для проведення всебічного дослідження проблеми міжнародної інформаційної безпеки. Мандатом Групи передбачається розгляд існуючих і потенційних загроз у сфері інформаційної безпеки та можливих спільних заходів щодо їхнього усунення, а також вивчення міжнародних концепцій, які були б спрямовані на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем.

Ще одним важливим етапом для розгляду питання міжнародної інформаційної безпеки став Усесвітній саміт з питань інформаційного суспільства (ВСІС) (World Summit on the Information Society (WSIS)) / *перший етап – 2003 р., Женева, другий етап – 2005 р., Туніс* /, який проходив під егідою ООН.

Проблематика міжнародної інформаційної безпеки увійшла до підсумкових документів женевської зустрічі ВСІС (WSIS) – Декларація принципів ВСІС "Побудова інформаційного суспільства: глобальний виклик у новому тисячолітті", Женева, 12 грудня 2003 (WSIS Declaration of Principles "Building the Information Society: a global challenge in the new Millennium" (WSIS-03/GENEVA/DOC/4-E, 12 December 2003)) [18] та План дій ВСІС Женева, 12 грудня 2003 (WSIS Plan of Action (WSIS-03/GENEVA/DOC/5-E, 12 December 2003)) [19]. У "Декларації принципів" зауважується, що міжнародна інформаційна безпека і безпека інформаційної інфраструктури є необхідною передумовою становлення глобального інформаційного суспільства та подолання асиметрії інформаційного розвитку. Проблема інформаційної безпеки у "Плані дій" розглядається в контексті конкретних заходів зі зміцнення довіри й безпеки при використанні інформаційно-комп'ютерних технологій (ІКТ), серед яких головну увагу приділено: поглибленню міжнародного співробітництва в рамках ООН і в межах інших міжнародних

ISSN 1728-3817

форумів з метою аналізу існуючих і потенційних інформаційних загроз; розробленню законодавства, що уможливлює ефективне розслідування неправомірного використання інформаційно-комп'ютерних технологій (ІКТ).

Подальший розвиток проблеми міжнародного співробітництва у сфері інформаційної безпеки знайшов своє втілення у політичних дискусіях і документах туніської зустрічі з інформаційного суспільства – ВСІС (Туніське зобов'язання), Туніс 18 листопада 2005 (WSIS Tunis Commitment (WSIS-05/TUNIS/DOC/7-E, 18 November 2005) [20] та WSIS Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6(Rev.1)-E,18 November 2005)) [21].

Під час туніської зустрічі виявилися гострі суперечності між підходами ООН і більшості держав – учасниць організації та США. У Туніському зобов'язанні (2005) було підтверджено позицію ООН щодо потенціалу інформаційно-комп'ютерних технологій (ІКТ) як чинника запобігання конфліктів, а також сприяння їх мирному врегулюванню. Разом із тим у Туніській програмі для інформаційного суспільства було підтримано ініціативу США та ряду держав стосовно упровадження стратегії глобальної культури кібербезпеки. Політико-правові аспекти глобальної культури кібербезпеки вбачаються у протидії кіберзлочинності, які вчинені в рамках юрисдикції однієї країни, але мають наслідки в інших, у необхідності дієвих і кваліфікованих інструментів і дій на національному й міжнародному рівнях. У програмі зроблено акцент на поглиблення співпраці у сфері інформаційної безпеки в рамках Азійсько-Тихоокеанського економічного співробітництво (АТЕС) (APEC) (Asia-Pacific Economic Cooperation (APEC)), Організації економічного співробітництва та розвитку (ОЕСР) (Organisation for Economic Co-operation and Development (OECD)) і Міжнародного союзу електрозв'язку (МСЕ) (International Telecommunication Union (ITU)), що демонструє комплексний підхід до протидії новітнім інформаційним загрозам на рівні законодавства.

Конференція запропонувала світовій спільноті розглянути існуючі й потенційні загрози для безпеки інформаційних і комунікаційних мереж, а також перспективну розробку міжнародної конвенції з інформаційної безпеки. Підґрунтям для такого рішення стали відповідні положення підсумкових документів регіональних конференцій з підготовки Всесвітньої зустрічі, а саме загальноєвропейської, азіатсько-тихоокеанської, африканської, західно-азійської та латиноамериканської, в яких було закладено основу для подальшого обговорення проблематики міжнародної інформаційної безпеки на рівні ООН.

Питання міжнародної інформаційної безпеки постійно обговорювалось на ГА ООН з метою розробки відповідного міжнародного документа на основі резолюцій: A/RES/60/51 (2005) [12] та A/RES/60/45 (2005) [13], в яких містилися положення про важливість протидії деструктивним впливам.

Отже, сьогоднішні реалії формують усе нові вимоги щодо розвитку інформаційного суспільства, а відповідно вимагають і нові уніфіковані нормативно-правові механізми й підходи з питань забезпечення безпеки інформаційного простору. Насамперед, це стосується розробки міжнародних принципів правового регулювання комунікаційних мереж. Саме в цьому напрямі І. Брацук та С. Кавин у своїх дослідженнях зауважують, що в контексті визначення інформаційної безпеки у відповідному міжнародному законодавстві можна зазначити, що в умовах глобалізації інформаційного простору акцент інформаційної безпеки припадає на сферу кібербезпеки. Це потребує якісно нової нормативної платформи для відносин у сфері інформаційної безпеки в рамках захисту національної безпеки й механізмів усунення загроз правовими засобами [27, с. 144].

На думку Метью С. Ваксман (Matthew C. Waxman), кібератаки – це національний потенціал, для якого міжнародне право та норми є невизначеними [31, с. 1–6]. Разом із тим, Б. Данкан Холліс (Duncan B. Hollis) зазначає, *що глобальні зусилля держав співпрацювати за допомогою міжнародних правил у боротьбі з кіберзагрозами дали, у кращому випадку, неоднозначні результати.* Як приклад, 2013 р. Група урядових експертів ООН (Group of Governmental Experts (UN GGE)) прийняла консенсусну доповідь, в якій зауважено, що "міжнародне право і, зокрема, Статут Організації Об'єднаних Націй, є застосовним і необхідним для підтримки миру, стабільності та сприяння відкритому, безпечному, середовищу інформаційно-комп'ютерних технологій (ІКТ)" [26, с. 147–159]. Цю позицію підтвердила інша GGE UN у 2015 р., яка також схвалила низку юридично необов'язкових норм відповідальної поведінки держави.

Із цього приводу І. Брацук та С. Кавин у статті "Нормативно-правові механізми забезпечення кібербезпеки в нових державах – членах ЄС" зазначають, *що необхідно активно сек'юризувати свій інформаційний простір і приділяти першочергову увагу захисту критично важливої інфраструктури як ключової умови національної безпеки. Власне такий формат гарантування інформаційної безпеки в контексті кіберзахисту диктує силовий підхід як найефективніший* [1, с. 36].

Відсутність ефективних міжнародних правових інструментів щодо кіберпростору в основному обговорювалася в теоретичних і політичних дебатах, які відображають з одного боку те, що держави повинні відігравати ключову та впливову роль у формуванні міжнародного права стосовно кіберпростору, з іншого те, що кіберпростір має залишатися вільним від будь-якого впливу й контролю. У цьому контексті Абід А. Адоніс (Abid A. Adonis) зауважує, *що такі дебати ґрунтуються на трьох основних викликах у формулюванні міжнародного права щодо кіберпростору, які пов'язані з основними принципами й характеристиками міжнародного публічного права: юрисдикція, арбітраж, правові інструменти та судова практика* [22, с. 1–5]. Інший науковець-правознавець Кубо Мачак (Kubo Mačák) зазначає, *що міжнародне право кібербезпеки на сьогодні перебуває у розпалі кризи: по-перше, пропозиції провідних зацікавлених сторін стосовно укладення міжнародно-обов'язкових договорів були зустрінуті окремими державами без особливого ентузіазму; по-друге, держави вкрай неохоче беруть на себе зобов'язання щодо конкретного тлумачення суперечливих правових питань і, таким чином, висловлюють свою opinio juris* [28, с. 1–13].

Відповідно на 72-й сесії ГА ООН 11 серпня 2017 р. було опубліковано доповідь Генерального секретаря ОНН (A/72/315) [7] як виконання рекомендацій Резолюції A/RES/71/28 від 5 грудня 2016 р. стосовно інформування країн про свою позицію з питань загального оцінювання міжнародної інформаційної безпеки й зусиль, які докладають держави. У цій промові були представлені офіційні звіти урядів 23 держав задля укріплення міжнародної безпеки та сприяння міжнародному співробітництву в цій сфері [14].

У цьому контексті, враховуючи поширення кіберзагроз, Генеральна Асамблея ООН 2019 р. ухвалила Резолюцію A/RES/74/28 (2019) [15], в якій підтверджується необхідність створення відкритого, безпечного, стабільного, доступного й мирного інформаційно-комунікаційного середовища, установлення довірчих відносин між державами, розширення можливостей країн щодо

співпраці та заохочення використання новітніх технологій. Це сприятиме зменшенню ризику виникнення конфліктів, що є суттєво важливою для забезпечення міжнародної безпеки. Разом із тим, Резолюцією A/RES/74/247 Генеральної Асамблеї ООН (27 грудня 2019 р.) [16] створено спеціальний міжурядовий комітет відкритого складу експертів і представників усіх регіонів для розроблення всеосяжної міжнародної конвенції про протидії використанню інформаційних і комунікаційних технологій зі злочинною метою. А в Резолюції ГА ООН A/RES/75/282 (26 травня 2021 р.) [17] було вирішено, що спеціальний комітет скличе принаймні шість сесій для завершення роботи над документом, щоб представити проєкт Конвенції на 78-й сесії Генеральної Асамблеї ООН (12–30 вересня 2023 р.). Тут можна виділити такі види міжнародної інформаційної безпеки, як глобальна інформаційна безпека; інформаційна безпека окремих держав у міжнародному інформаційному просторі; інформаційна безпека установ у міжнародному інформаційному просторі тощо. Ці види інформаційної безпеки зазначені і в документах ООН [8], [10].

Висновки. Необхідність створення міжнародних актів, які містили б уніфіковані норми із правового регулювання міжнародної інформаційної безпеки, продиктовані глобальним розвитком сучасного інформаційного суспільства. Саме безпека на інформаційному рівні часто є пріоритетною для країни, оскільки визначає, з одного боку, рівень захищеності та, як наслідок, стійкості основних сфер життєдіяльності суспільства (країни) щодо небезпечного інформаційного впливу, а з іншого – інтенсивність розвитку суспільства в тій чи іншій сфері за рахунок ефективного використання накопичених знань.

У сфері гарантування інформаційної безпеки на національному й міжнародному рівні необхідно продовжити та розширити діяльність зі створення умов для формування системи міжнародної інформаційної безпеки на основі загальновизнаних принципів і норм міжнародного права. Зокрема на рівні ООН необхідно підготувати й ухвалити міжнародно-правові акти, що регламентують застосування принципів і норм міжнародного права у сфері використання інформаційних та комунікаційних технологій.

Оскільки єдиного глобального акту, який регламентує порядок протидії інформаційним загрозам, як зовнішнім, так і внутрішнім немає, то в цьому контексті дуже важливою є питання розроблення Конвенції ООН про забезпечення міжнародної інформаційної безпеки, в якій необхідно було би закріпити таке: основні загрози міжнародному миру й безпеці в інформаційному просторі; основні засади забезпечення міжнародної інформаційної безпеки; детально прописати принципи міжнародного співробітництва в боротьбі зі злочинами в інформаційній галузі; визначити ефективні та дієві механізми правової відповідальності в інформаційному просторі аж до створення спеціального міжнародного органу щодо розслідування злочинів в інформаційній сфері.

Список використаних джерел

1. Кавин С. Нормативно-правові механізми забезпечення кібербезпеки в нових державах – членах ЄС / С. Кавин, І. Брацук // Вісн. Київ. нац. ун-ту імені Тараса Шевченка. Юридичні науки. – 2021. – № 2 (117). – С. 30–38.
2. Копійка М. В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки / М. В. Копійка // Політичне життя. – 2020. – № 1. – С. 102–109.
3. Міжнародна інформаційна безпека: теорія і практика: підручник / Є. А. Макаренко, М. М. Рижков, М. А. Ожеван та ін. – Київ: Центр вільної преси, 2016. – 418 с.
4. Ожеван М. А. Глобальна війна гранд-наративів у сучасну добу. Стратегічні комунікації в міжнародних відносинах : монографія / М. А. Ожеван. – К. : Вадекс, 2019. – 442 с.
5. Developments in the field of information and telecommunications in the context of international security" : report of the Secretary-General (A/55/140) 10 July 2000 [Electronic resource]. – Access mode: https://digitallibrary.un.org/search?ln=ru&p=%20A%2F55%2F140&f=&c=Resource%20Type&c=UN%20Bodies&sf=&so=d&rg=50&fti=0 (дата звернення: 15.12.2022)
6. Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General (A/56/164/Add.1) 3 October 2001 [Electronic resource]. – Access mode: https://digitallibrary.un.org/record/449994? (дата звернення: 15.12.2022)
7. Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General (A/72/315) 11 August 2017 [Electronic resource]. – Access mode: https://digitallibrary.un.org/record/1305217? (дата звернення: 15.12.2022)
8. Resolution adopted by the General Assembly [on the report of the First Committee (A/53/576)] 53/70 4 January 1999. Developments in the field of information and telecommunications in the context of international security [Electronic resource]. – Access mode: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement (дата звернення:15.12.2022)
9. Resolution adopted by the General Assembly [on the report of the First Committee (A/54/559)] 54/50 23 December 1999. Role of science and technology in the context of international security and disarmament [Electronic resource]. – Access mode: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/19/PDF/N9977719.pdf?OpenElement (дата звернення: 15.12.2022)
10. Resolution adopted by the General Assembly [on the report of the First Committee (A/55/554)] 55/28 20 December 2000. Developments in the field of information and telecommunications in the context of international security [Electronic resource]. – Access mode: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561/07/PDF/N0056107.pdf?OpenElement (дата звернення: 15.12.2022)
11. Resolution adopted by the General Assembly [on the report of the First Committee (A/56/533)] 56/19 7 January 2002. Developments in the field of information and telecommunications in the context of international security [Electronic resource]. – Access mode: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/28/PDF/N0147628.pdf?OpenElement (дата звернення: 15.12.2022)
12. Resolution adopted by the General Assembly on 8 December 2005 [on the report of the First Committee (A/60/459)] 60/51. Role of science and technology in the context of international security and disarmament [Electronic resource]. – Access mode: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/490/66/PDF/N0549066.pdf?OpenElement (дата звернення: 15.12.2022)
13. Resolution adopted by the General Assembly on 8 December 2005 [on the report of the First Committee (A/60/452)] 60/45. Developments in the field of information and telecommunications in the context of international security [Electronic resource]. – Access mode: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/490/30/PDF/N0549030.pdf?OpenElement (дата звернення: 15.12.2022)
14. Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)] 73/266. Advancing responsible State behaviour in cyberspace in the context of international security [Electronic resource]. – Access mode: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement (дата звернення: 15.12.2022)
15. Resolution adopted by the General Assembly on 12 December 2019 [on the report of the First Committee (A/74/363)] 74/28. Advancing responsible State behaviour in cyberspace in the context of international security [Electronic resource]. – Access mode: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/00/PDF/N1941000.pdf?OpenElement (дата звернення: 15.12.2022)
16. Resolution adopted by the General Assembly on 27 December 2019 [on the report of the Third Committee (A/74/401)] 74/247. Countering the use of information and communications technologies for criminal purposes [Electronic resource]. – Access mode: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement (дата звернення: 15.12.2022)
17. Resolution adopted by the General Assembly on 26 May 2021 [without reference to a Main Committee (A/75/L.87/Rev.1 and A/75/L.87/Rev.1/Add.1)] 75/282. Countering the use of information and communications technologies for criminal purposes [Electronic resource]. – Access mode: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement (дата звернення: 15.12.2022)
18. WSIS Declaration of Principles "Building the Information Society: a global challenge in the new Millennium" (WSIS-03/GENEVA/DOC/4-E, 12 December 2003 [Electronic resource]. – Access mode: https://www.itu.int/net/wsis/docs/geneva/official/dop.html (дата звернення: 10.12.2022)
19. WSIS Plan of Action (WSIS-03/GENEVA/DOC/5-E, 12 December 2003 [Electronic resource]. – Access mode: https://www.itu.int/net/wsis/docs/geneva/official/poa.html (дата звернення: 10.12.2022)
20. WSIS Tunis Commitment (WSIS-05/TUNIS/DOC/7-E, 18 November 2005 [Electronic resource]. – Access mode: https://www.itu.int/net/wsis/docs2/tunis/off/7.html (дата звернення: 10.12.2022)
21. WSIS Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2005 [Electronic resource]. – Access mode: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (дата звернення: 10.12.2022)
22. Abid A. Adonis International Law on Cyber Security in the Age of Digital Sovereignty E-International Relations Mar 14 2020

ISSN 1728-3817

23. Information security: A review of information security issues and techniques / F. Alkhudhayr, S. Alfarraj, B. Aljameeli, S. Elkhdiri In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). – P. 1–6.
24. Brent L. NATO's role in cyberspace / L. Brent // The Three Swords Magazine. – 2019. – Vol. 34. – P. 56–59.
25. Cebrovski A. Network – Centric Warfare: Its Origin and Future / A. Cebrovski, J. Garstka // Proceedings. – 1998, January. – Vol. 124/1/1, 139.
26. Duncan B. Hollis. Waxman Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative (PSI) Temple University Beasley School of Law / B. Hollis Duncan, C. Matthew // Legal studies research paper. – 2018. – No. 26. – 03 January.
27. Kavyn Sviatoslav. Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France / Sviatoslav Kavyn, Ivan Bratsuk // Teise. – 2021. – Vol. 121. – P. 135–147.
28. Kubo Mačák Is the International Law of Cyber Security in Crisis? 2016 8th International Conference on Cyber Conflict Cyber Power / N. Pissanidis, H. Rõigas, M. Veenendaal (Eds.). – 2016. NATO CCD COE Publications, Tallinn
29. Libicki M. C. Conquest in Cyberspace: National Security and Information Warfare / M. C. Libicki. – Cambridge: Cambridge University Press, 2007. – 336 p.
30. Nye J. S. Cyber Power / Joseph S. Nye. – Cambridge: Pub. by Belfer Center for Science and International Affairs, 2010. – 26 p.
31. Matthew C. Waxman Cyber Strategy & Policy: International Law Dimensions Written Testimony Before the Senate Armed Services Committee March 2, 2017.
32. Mukundan N. R. Perceived information security of internal users in Indian IT services industry / N. R. Mukundan, Sai L. Prakash // Information Technology and Management. – 2014. – № 15(1). – pp. 1–8.
33. Potejko P. Information security in: Wojtaszczyk, K., Materska-Sosnowska, A. (ed.), State security. ASPRA-JR publishing house, Warsaw, 2009. – 194 p.

References

1. Kavyn S., Ya., Bratsuk I. Zn. (2021) Normatyvno-pravovi mekhanizmy zabezpechennia kiberbezpeky v novykh derzhavakh – chlenakh YeS [Regulatory And Legal Implemantation Of Cyber Security As A Component Of Information Security In The Countries Of Central And Eastern Europe] Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Yurydychni nauky [Bulletin of Taras Shevchenko National University of Kyiv. Legal Studies], 2(117), 30–38 (in Ukrainian)
2. Kopiika M. V. (2020) Modernizatsiia polityky mizhnarodnykh orhanizatsii u sferi informatsiinoi bezpeky [Modernization of the policy of the international organizations in information security] Politychne zhyttia [Political Life], 1, 102–109 (in Ukrainian)
3. Makarenko I. A., Ryzhkov M. M., Ozhevan M., Kuchmii O. P., Frolova O. M. (2016) Mizhnarodna informatsiina bezpeka: teoriia i praktyka [International information security: theory and practice] Pidruchnyk. – Kyiv: Free press center, 418 p. (in Ukrainian)
4. Ozhevan M. (2019) Hlobalna viina Hrand-naratyviv u suchasnu dobu // Stratehichni komunikatsii v mizhnarodnykh vidnosynakh. Monohrafiia [The global war of grand narratives in the modern times // Strategic communications in international relations] Monohrafiia – Kyiv: Vadeks, 442 p. (pp. 60–96) (in Ukrainian)
5. Developments in the field of information and telecommunications in the context of international security" : report of the Secretary-General (A/55/140) 10 July 2000 URL: https://digitallibrary.un.org/search?ln=ru&p=%20A%2F55%2F140&f=&c=Resource%20Type&c=UN%20Bodies&sf=&so=d&rg=50&fti=0 (data zvernennia: 15.12.2022) (in English)
6. Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General A/56/164/Add.1 3 October 2001 URL: https://digitallibrary.un.org/record/449994?ln (data zvernennia: 15.12.2022) (in English)
7. Developments in the field of information and telecommunications in the context of international security: report of the Secretary-General A/72/315 11 August 2017 URL: https://digitallibrary.un.org/record/1305217?ln (data zvernennia: 15.12.2022) (in English)
8. Resolution adopted by the General Assembly [on the report of the First Committee (A/53/576)] 53/70 4 January 1999. Developments in the field of information and telecommunications in the context of international security URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement (data zvernennia: 15.12.2022) (in English)
9. Resolution adopted by the General Assembly [on the report of the First Committee (A/54/559)] 54/50 23 December 1999. Role of science and technology in the context of international security and disarmament URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/777/19/PDF/N9977719.pdf?OpenElement (data zvernennia: 15.12.2022) (in English)
10. Resolution adopted by the General Assembly [on the report of the First Committee (A/55/554)] 55/28 20 December 2000. Developments in the field of information and telecommunications in the context of international security URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561/07/PDF/N0056107.pdf?OpenElement (data zvernennia: 15.12.2022) (in English)
11. Resolution adopted by the General Assembly [on the report of the First Committee (A/56/533)] 56/19 7 January 2002. Developments in the field of information and telecommunications in the context of international security URL:https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/28/PDF/N0147628.pdf?OpenElement (data zvernennia: 15.12.2022) (in English)
12. Resolution adopted by the General Assembly on 8 December 2005 [on the report of the First Committee (A/60/459)] 60/51. Role of science and technology in the context of international security and disarmament URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/490/66/PDF/N0549066.pdf?OpenElement (data zvernennia: 15.12.2022) (in English)
13. Resolution adopted by the General Assembly on 8 December 2005 [on the report of the First Committee (A/60/452)] 60/45. Developments in the field of information and telecommunications in the context of international security URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/490/30/PDF/N0549030.pdf?OpenElement (data zvernennia: 15.12.2022) (in English)
14. Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)] 73/266. Advancing responsible State behaviour in cyberspace in the context of international security URL:https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement (data zvernennia: 15.12.2022) (in English)
15. Resolution adopted by the General Assembly on 12 December 2019 [on the report of the First Committee (A/74/363)] 74/28. Advancing responsible State behaviour in cyberspace in the context of international security URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/410/00/PDF/N1941000.pdf?OpenElement (data zvernennia: 15.12.2022) (in English)
16. Resolution adopted by the General Assembly on 27 December 2019 [on the report of the Third Committee (A/74/401)] 74/247. Countering the use of information and communications technologies for criminal purposes URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement (data zvernennia: 15.12.2022) (in English)
17. Resolution adopted by the General Assembly on 26 May 2021 [without reference to a Main Committee (A/75/L.87/ Rev. 1 and A/75/L.87/Rev.1/Add.1)] 75/282. Countering the use of information and communications technologies for criminal purposes URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement (data zvernennia: 15.12.2022) (in English)
18. WSIS Declaration of Principles "Building the Information Society: a global challenge in the new Millennium" (WSIS-03/GENEVA/DOC/4-E, 12 December 2003 URL: https://www.itu.int/net/wsis/docs/geneva/official/dop.html (data zvernennia: 10.12.2022) (in English)
19. WSIS Plan of Action (WSIS-03/GENEVA/DOC/5-E, 12 December 2003 URL: https://www.itu.int/net/wsis/docs/geneva/official/poa.html (data zvernennia: 10.12.2022) (in English)
20. WSIS Tunis Commitment (WSIS-05/TUNIS/DOC/7-E, 18 November 2005 URL: https://www.itu.int/net/wsis/docs2/tunis/off/7.html (data zvernennia: 10.12.2022) (in English)
21. WSIS Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2005 URL: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (дата звернення: 10.12.2022) (in English)
22. Abid A. Adonis International Law on Cyber Security in the Age of Digital Sovereignty E-International Relations Mar 14 2020
23. Alkhudhayr F., Alfarraj S., Aljameeli B., Elkhdiri S. Information security: A review of information security issues and techniques. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). P. 1–6.
24. Brent L. NATO's role in cyberspace. The Three Swords Magazine 34/2019. P. 56-59.
25. Cebrovski A., Garstka J. Network – Centric Warfare: Its Origin and Future / A. Cebrovski, J. Garstka // Proceedings. January 1998. Vol. 124/1/1, 139.
26. Duncan B. Hollis, Matthew C. Waxman Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative (PSI) Temple University Beasley School of Law Legal studies research paper NO. 2018-03 January 26, 2018.
27. Sviatoslav Kavyn, Ivan Bratsuk, Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France // Teise. – 2021. –Vol. 121. – P. 135–147
28. Kubo Mačák Is the International Law of Cyber Security in Crisis? 2016 8th International Conference on Cyber Conflict Cyber Power N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.) 2016. NATO CCD COE Publications, Tallinn
29. Libicki M.C. Conquest in Cyberspace: National Security and Information Warfare / M. C. Libicki. – Cambridge: Cambridge University Press, 2007. – 336 p.
30. Nye J.S. Cyber Power / Joseph S. Nye. – Cambridge: Pub. by Belfer Center for Science and International Affairs, 2010. – 26 p.
31. Matthew C. Waxman Cyber Strategy & Policy: International Law Dimensions Written Testimony Before the Senate Armed Services Committee March 2, 2017
32. Mukundan N. R., Prakash Sai L. Perceived information security of internal users in Indian IT services industry. Information Technology and Management. 2014. № 15 (1). P. 1–8.
33. Potejko P. Information security in: Wojtaszczyk, K., Materska-Sosnowska, A. (ed.), State security, ASPRA-JR publishing house, 2009.Warsaw, 194 p.

Надійшла до редколегії 27.02.23

I. Bratsuk, PhD (Law), Associate Prof.
ORCID ID: 0000-0003-0164-7407,
S. Kavyn, PhD Student
ORCID ID: 0000-0002-6189-3848
Ivan Franko National University of Lviv, Lviv, Ukraine

INTERNATIONAL LEGAL REGULATION OF ENSURING INFORMATION SECURITY WITHIN THE FRAMEWORK OF THE UN

As a result of the active implementation of digital technologies in all spheres of social life, both international and national legal mechanisms aiming at ensuring the support for the security of the information space stand out in the foreground. The existing legal mechanisms provide for the improvement and harmonization of the legal framework in the field of information security at the national and international levels. In this context, the idea of digital sovereignty determines the use of legal mechanisms that ensure the protection of information security. Due to this faction, a comprehensive study of the general patterns of functioning and development of international legal mechanisms for ensuring information security within the framework of the UN is particularly appropriate, relevant and requires a detailed analysis.

The article addresses the analysis and study of UN legal mechanisms in the field of ensuring information security. The purpose of the scientific work is a comprehensive study of the general patterns of functioning and development of international legal mechanisms for ensuring information security within the framework of the UN and the development of scientifically based proposals and recommendations regarding the effective operation of these mechanisms in international and national legal orders (legal systems). The methodological basis of scientific research is general scientific and special legal methods. In particular, a systematic approach, a generalization method, and a systematic analysis were used in the process of scientific research. In the course of the study, there were analyzed: the peculiarities of the functioning of the institutional and legal mechanism of information protection within the framework of UN coordination in the context of the multi-vector system of international security and legal regulation of international cooperation. The article substantiates the expediency of developing an integrated, coordinated information policy of international organizations and institutions with the aim of unifying approaches to ensuring information security. Also, the work summarizes the main problems arising in the international legal regulation of the fight in the field of ensuring information security, and the main threats to international peace and security in the information space, and suggests as well ways to solve them. In this context, the work summarizes the principles of international information security, highlights the main trends in the development of cyber threats in the modern information space and measures necessary for their neutralization. The article analyzes the peculiarities of the functioning of the institutional and legal mechanism of cyber protection in the context of the legislative regulation of international cooperation between international organizations and institutions. In particular, an analysis of the main mechanisms of legal support for cyber protection of the information space was carried out with the aim of their integration into a unified international system of the legal information field. As a result of the study, recommendations were formed. In the field of ensuring information security at the national and international levels, it is necessary to continue and expand activities to create conditions for the formation of an international information security system based on generally recognized principles and norms of international law. In particular, at the UN level, it is necessary to prepare and adopt international legal acts regulating the application of the principles and norms of international law in the field of the use of information and communication technologies. Since there is no single global act that regulates the procedure for combating information threats, in this context, the task of developing the UN Convention on International Information Security is very important. The document should: identify the main threats to international peace and security in the information space; determine the main principles of ensuring international information security; prescribe in detail the principles of international cooperation in the fight against crimes in the information sphere; determine effective and efficient mechanisms of legal responsibility in the information space up to the creation of a special international body for the investigation of crimes in the information sphere.

Keywords: international information security, international law, international organizations, the UN, international legal acts, resolution, legal mechanisms, conventions.