

УДК 341.45

DOI <https://doi.org/10.24144/2788-6018.2023.01.100>

МЕХАНІЗМ СПІВРОБІТНИЦТВА ДЕРЖАВ ЩОДО ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Ковалів С.В.,

кандидат юридичних наук, професор,
завідувач кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ,
ORCID ID: 0000-0002-9730-8401

Єсімов С.С.,

кандидат юридичних наук, доцент
професор кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ,
ORCID ID: 0000-0002-9327-0071

Ковалів С.В., Єсімов С.С. Механізм співробітництва держав щодо протидії злочинам у сфері інформаційних технологій.

У статті розглянуто механізм співробітництва держав щодо протидії злочинам у сфері інформаційних технологій. Для дослідження використано загально-наукові методи пізнання – формально-логічний, системно-структурний, а також приватно наукові методи – формально-юридичний та порівняльно-правовий. Міжнародне співробітництво з протидії злочинам у сфері інформаційних та комунікаційних технологій є актуальним для України, яка активно виступає за зміцнення міждержавної взаємодії в галузі, що розглядається. Дослідження внеску Організації Об'єднаних Націй у розвиток правових та інституційних основ протидії злочинам у сфері інформаційних технологій має значення для всіх сфер суспільного життя. Вказано, що проблематика протидії злочинам у сфері інформаційних технологій є комплексною, у зв'язку з чим активно вивчається фахівцями різних галузей науки. Водночас, низка ключових аспектів міжнародно-правового регулювання співробітництва держав щодо протидії злочинам у сфері інформаційних технологій залишалася без комплексної міжнародно-правової оцінки. Функціонування інституційного механізму ООН щодо протидії злочинам у сфері інформаційних технологій здійснюється з урахуванням зростаючої необхідності реалізації ефективної міжнародної співпраці, збільшення ролі нормативно-правових засад міждержавної взаємодії. Розглянуто діяльність структурних підрозділів Організації Об'єднаних Націй, які здійснюють протидію злочинності у сфері інформаційних технологій. Особлива увага приділена діяльності Міжнародного союзу електрозв'язку та його вкладу у захист дітей від деструктивного впливу у мережі Інтернет і проведення заходів направлених на протидію злочинності у сфері інформаційних технологій. Розгля-

нуто діяльність Конгресів Організації Об'єднаних Націй з попередження злочинності та кримінального правосуддя та їх вплив на формування нормативно-правового забезпечення протидії злочинності у сфері інформаційних технологій. Визначено тенденції, які безпосередньо впливають на стан кіберзлочинності та розкрито заходи, які вживаються міжнародними організаціями у складі ООН з метою протидії злочинності у сфері інформаційних технологій.

Ключові слова: міжнародне співробітництво, інституційний механізм, міжнародний правовий акт, інформаційно-комунікаційні технології, злочинність.

Kovaliv S.V., Yesimov S.S. The mechanism of cooperation of states in combating crimes in the field of information technologies.

The article examines the mechanism of cooperation between states in combating crimes in the field of information technologies. The research used general scientific methods of cognition - formal-logical, systemic-structural, as well as private scientific methods - formal-legal and comparative-legal. International cooperation in combating crimes in the field of information and communication technologies is relevant for Ukraine, which is actively advocating for the strengthening of interstate cooperation in the field under consideration. The study of the contribution of the United Nations to the development of legal and institutional frameworks for countering crimes in the field of information technologies is important for all spheres of public life. It indicated that the problems of combating crimes in the field of information technologies are complex, and in connection with this, specialists in various fields of science actively study them. At the same time, a number of key aspects of the international legal regulation of cooperation between states

in combating crimes in the field of information technologies remained without a comprehensive international legal assessment. The functioning of the UN institutional mechanism for countering crimes in the field of information technologies carried out taking into account the growing need to implement effective international cooperation, increasing the role of regulatory and legal bases of interstate cooperation. The activity of structural divisions of the United Nations Organization, which carry out countermeasures against crime in the field of information technologies, is considered. Special attention paid to the activities of the International Telecommunication Union and its contribution to the protection of children from the destructive influence of the Internet and the implementation of measures aimed at countering crime in the field of information technologies. The activities of the Congresses of the United Nations Organization on crime prevention and criminal justice and their influence on the formation of regulatory and legal protection against crime in the field of information technologies are considered. The trends that directly affect the state of cybercrime identified and the measures taken by international organizations within the UN to combat crime in the field of information technologies disclosed.

Key words: international cooperation, institutional mechanism, international legal act, information and communication technologies, crime.

Постановка проблеми. У умовах розвитку міжнародного співробітництва у боротьбі зі злочинністю важливого значення набувають інституційні механізми протидії злочинам у сфері інформаційних технологій сформовані Організацією Об'єднаних Націй. Інституційний механізм розглядається як сукупність компетентних підрозділів різних міжнародних організацій, які беруть участь у міжнародному співробітництві з протидії злочинам у сфері інформаційних технологій. Кожен механізм включає певну кількість структурних елементів органів, агентств, міжнародних центрів та вносить вклад у формування засад протидії злочинності у сфері використання інформаційних технологій.

Стан опрацювання проблематики. Співробітництву держав з протидії злочинам у сфері інформаційних технологій посвячені праці: Ю.В. Батуріна, В.В. Бута, О.Г. Волеводза, В.Д. Гавловського, В.О. Голубева, М.В. Гуцалюка, М.С. Дашян, В.М. Дрьоміна, Н.А. Зелінської, І.М. Забари, В.В. Кравчука, Б.В. Романюка, В.С. Цимбалюка та інших вчених. Прагнення України до вступу в Європейський Союз ставлять завдання з посилення інформаційної безпеки, впровадження міжнародних стандартів з метою уніфікації систем захисту та посилення протидії злочинності у сфері інформаційних технологій.

Метою статті є дослідження механізму співробітництва держав щодо протидії злочинам у сфері інформаційних технологій.

Виклад основного матеріалу. Ключові напрями міждержавної взаємодії у сфері співробітництва держав щодо протидії злочинам у сфері інформаційних технологій в досліджуваній галузі були сформульовані в Резолюції Генеральної Асамблеї 53/70 від 4 грудня 1998 року «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» та включали: загальну оцінку проблем інформаційної безпеки; визначення основних понять, що стосуються інформаційної безпеки, включаючи неправомірне використання інформаційно-комунікаційних систем і інформаційних ресурсів; розробку міжнародних принципів, які спрямовані на зміцнення безпеки глобальних інформаційних та комунікаційних систем та сприяли боротьбі з інформаційним криміналом [1].

В.В. Попко зазначає, що забезпечення кібербезпеки, дотримання прав людини та захист важливої інформаційної інфраструктури вимагають від держав значних зусиль на національному та на міжнародному рівнях [2, с. 282].

У 2004 році в ООН створено Групу урядових експертів у сфері інформатизації та комунікацій, основним завданням, якої став розгляд існуючих і потенційних загроз у сфері інформаційної безпеки та розробку заходів щодо усунення на підставі інформації, що надається державами-членами. Група здійснює обмін думками щодо подій у галузі інформації та комунікацій у контексті міжнародної безпеки, готує доповіді за результатами роботи, в яких відображає актуальні загрози в галузі інформатизації та комунікацій, пропонує заходи боротьби та формулює рекомендації.

У 2018 році Генеральною Асамблеєю ООН прийнято чергову резолюцію «Досягнення в сфері інформатизації та телекомунікацій у контексті міжнародної безпеки», яка передбачала створення Робочої групи з міжнародної інформаційної безпеки відкритого складу, розрахованої на участь усіх держав-членів ООН та проведення міжсесійних консультацій з приватними партнерами та науковою спільнотою.

Контртерористичний комітет ООН робить внесок у протидію використанню інформаційних технологій для здійснення терористичної діяльності, фінансування терористичних актів, вербування нових членів терористичних угруповань. Робота зазначеної структури зосереджена на напрямках: оцінка виконання державами-членами ООН резолюцій щодо злочинного використання інформаційних технологій; сприяння міжнародному співробітництву у протидії інформаційним загрозам; зміцнення співробітництва з надання правової допомоги щодо цифрового контенту; розвиток обміну інформацією.

Антитерористичний підрозділом ООН – Контртерористичне управління реалізує низку ініціатив у сфері інформаційних технологій. Програма з кібербезпеки та використання нових технологій, спрямована на розширення можливостей держав-членів ООН та приватних партнерів щодо запобігання та пом'якшення наслідків неправомірного використання інформаційно-комунікаційних технологій. Програма включає розвиток співпраці з протидії загрози кібератак на об'єкти критичної інформаційної інфраструктури, використання соціальних мереж для збирання інформації з відкритих джерел та доказів з використання інформаційних технологій.

Актуальність Програми зазначена у шостому огляді Глобальної контртерористичної стратегії ООН, що відображено у відповідній резолюції Генеральної асамблеї ООН та Доповіді Генерального секретаря ООН [3].

Інституційний механізм ООН щодо протидії злочинам в інформаційній сфері включає Управління по боротьбі з наркотиками та злочинністю, що сприяє довгостроковому посиленню потенціалу держав у боротьбі з кіберзлочинністю, сприяючи компетентним національним правоохоронним органам у формуванні ефективних заходів реагування.

В Управлінні по боротьбі з наркотиками та злочинністю ООН сформувалися спеціалізовані структури для розвитку співробітництва у боротьбі зі злочинами у сфері інформаційних технологій. Група експертів для проведення дослідження проблеми кіберзлочинності, заснована відповідно п. 42 Сальвадорської декларації про комплексні стратегії для відповіді на глобальні виклики: системи запобігання злочинності та кримінального правосуддя з метою проведення дослідження проблеми кіберзлочинності, заходів реагування на її прояви з боку держав-членів, міжнародної спільноти та приватних партнерів [4].

Значення роботи Групи експертів полягає в тому, що вперше на міжнародному рівні було проведено всебічне дослідження з метою вивчення можливих шляхів зміцнення існуючих та вироблення пропозицій щодо нових національних та міжнародних правових заходів щодо протидії кіберзлочинності. Унікальність проведеної роботи у тому, що вона охопила проблематику кіберзлочинності та зв'язок з іншими видами злочинів. Аналіз багаторічної роботи Групи експертів дозволяє зробити висновки: зростає необхідність реалізації ефективного та ширшого регіонального та міжнародного співробітництва у боротьбі з кіберзлочинністю; ключове значення у сфері протидії кіберзлочинності мають нормативно-правові засади, можливості правоохоронних органів та міжнародне співробітництво; погроза кіберзлочинності пов'язана з транснаціональною організованою злочинністю, у тому числі з тероризмом,

виникла необхідність у відповідності положень про криміналізацію, процесуальні повноваження правоохоронних органів, про питання визначення юрисдикції та забезпечення безпеки електронних доказів; зростає потреба в реалізації оперативного та ефективного реагування на запити про взаємну правову допомогу, яка стосується збереження та отримання електронних доказів; виникла потреба у вирішенні питань юрисдикції щодо хмарних технологій; особливу значимість набуває розвиток мережевої взаємодії з метою обміну досвідом для вирішення проблем, що виникають у зв'язку з різницею національних вимог щодо прийнятності, доказової сили, цілісності та достовірності електронних доказів.

Відповідно до плану роботи Групи експертів на 2018–2022 роки найбільш пріоритетним напрямом була діяльність щодо предметних обговорень передових практик держав-членів ООН у сфері протидії кіберзлочинності за участю приватних партнерів та представників наукової спільноти.

Відповідно до резолюції Генеральної Асамблеї ООН 74/247 від 27 грудня 2019 року засновано Спеціальний міжурядовий комітет експертів відкритого складу для розробки міжнародної конвенції про протидію використанню інформаційно-комунікаційних технологій у злочинних цілях.

Спеціальний міжурядовий комітет має представляти всі регіони та розробляти проект конвенції з урахуванням існуючих міжнародних інструментів, враховуючи результати діяльності Групи експертів для проведення дослідження проблеми кіберзлочинності [5].

Діяльність Спеціального міжурядового комітету побудована з урахуванням досвіду розробки Конвенції ООН проти транснаціональної організованої злочинності та Конвенції ООН проти корупції. Для вирішення глобального завдання розробки конвенції планується проведення восьми сесій у Відні у 2024 році та подання тексту конвенції у вигляді проекту резолюції Генеральної Асамблеї ООН для розгляду та прийняття на сімдесят дев'ятій сесії у тому же році.

На офіційних сесіях Спеціального комітету, держави-члени проводять неофіційні консультації з метою досягнення консенсусу з питань, пов'язаних із розробкою конвенції. Увага приділяється забезпеченню прозорості переговорного процесу та участі максимальної кількості держав-членів.

ООН має прагнення до сімдесят дев'ятої сесії Генеральної Асамблеї у 2024 році розробити комплексний міжнародний договір щодо протидії використанню інформаційно-комунікаційних технологій у злочинних цілях з урахуванням чинних міжнародних документів.

На думку М. О. Семко, аналіз резолюцій ГА ООН з 1998 по 2021 рік дає змогу прийти до висновків, що ООН не вбачає нагальної потреби у

створенні системи конкретних міжнародних норм, які б створювали єдиний механізм забезпечення міжнародної інформаційної безпеки у військовій сфері та під час збройних конфліктів [6].

Міжнародний союз електрозв'язку – спеціалізована установа ООН у галузі інформаційних технологій, приймає участь у протидії злочинам у сфері інформаційних технологій. Діяльність спрямована на вирішення питань технологій, послуг та розподілу глобальних ресурсів радіочастотного спектру та супутникових орбітальних позиції з метою створення єдиної глобальної системи зв'язку, яка постійно розвивається.

Міжнародний союз електрозв'язку реалізує Програму кібербезпеки, яка надає державам-членам можливості підвищення рівня кібербезпеки на національному рівні. Відповідно до Програми Міжнародний союз електрозв'язку розраховує Глобальний індекс кібербезпеки, який дозволяє проаналізувати рівень готовності держав до забезпечення різних аспектів кібербезпеки. При розрахунку Глобального індексу кібербезпеки враховуються правові, технічні і організаційні заходи забезпечення кібербезпеки, заходи щодо розвитку міжнародного співробітництва у цій сфері.

Глобальний індекс кібербезпеки включає 25 показників, за якими здійснюється моніторинг діяльності держав щодо п'яти напрямів забезпечення кібербезпеки. Глобальний індекс кібербезпеки свідчить про розвиток тенденції посилення кібербезпеки, проте вказує, що спостерігається наявність цифрового розриву між державами. Міжнародний союз електрозв'язку публікує результати діяльності національних органів держав у сфері протидії злочинності у сфері інформаційно-комунікаційних технологій.

Однією з ініціатив Міжнародного союзу електрозв'язку є захист дітей в мережі Інтернет. Союз розробив Керівні настанови щодо захисту дитини в цифровому середовищі. Нові Рекомендації (2020) були заново усвідомлені, сформульовані й перебудовані з урахуванням значних змін, що відбулися в цифровому середовищі, в якому живе сьгоднішнє покоління дітей. Окрім додання нових розробок у сфері цифрових технологій та платформ, у цьому новому виданні була усунута значна прогалина: приділяється увага становищу дітей-інвалідів, для яких цифрове середовище відкриває особливо важливі можливості щодо забезпечення повноцінної участі в соціальному житті [7, с. III].

Ключовими завданнями у сфері захисту дітей в мережі Інтернет є: виявлення загроз у кіберпросторі; підвищення обізнаності; розробка практичних заходів щодо мінімізації загроз; обмін досвідом; розробка стратегій забезпечення безпеки у мережі Інтернет, що охоплюють п'ять ключових галузей: правові заходи; технічні заходи; органі-

заційні заходи; сприяння державам у здійсненні обміну досвідом щодо захисту дітей в Інтернеті; міжнародна співпраця.

Міжнародний союз електрозв'язку опублікував Керівництво з питань національної стратегії у галузі кібербезпеки з метою сприяння державам у розробці та впровадженні національних стратегій кібербезпеки. Основною метою розробки Керівництва є створення моделі стратегії кібербезпеки, зміцнення довіри у процесі використання інформаційних технологій. Дотримання рекомендацій, сформульованих у Керівництві, дозволяє врахувати специфічну ситуацію в кожній державі, культурні та суспільні цінності, забезпечити безпечний розвиток транснаціональних комунікаційних процесів та інформаційних технологій [8].

Питання протидії злочинам у сфері інформаційних технологій активно обговорюються на Конгресах ООН з попередження злочинності та кримінального правосуддя. Вперше питання боротьби зі злочинами, пов'язаними з використанням комп'ютерної мережі, обговорювалися на десятому Конгресі ООН. На одинадцятому Конгресі ООН держави-члени підтвердили значущість розробки національних заходів та розвитку міжнародного співробітництва з протидії кіберзлочинності, зазначено, що активний розвиток інформаційних технологій супроводжується використанням у злочинних цілях, у зв'язку з чим зростає необхідність міждержавної взаємодії у попередженні та розслідуванні злочинів пов'язаних із використанням інформаційних технологій, притягнення винних осіб до відповідальності.

На дванадцятому Конгресі ООН проблема протидії кіберзлочинності розглядалася як основне питань порядку денного. На тринадцятому Конгресі ООН держави-члени приділяли особливу увагу розробці конкретних заходів, спрямованих на створення захищеного кіберпростору; попередженню та припиненню злочинної діяльності, що здійснюється з використанням інформаційних технологій; зміцнення співпраці між компетентними правоохоронними органами; підвищенню захищеності комп'ютерних мереж та забезпечення їх захисту; зміцнення здатності національних відомств протидіяти кіберзлочинності за допомогою профілактики, виявлення та розслідування злочинів.

Відповідно до порядку денного чотирнадцятого Конгресу ООН з попередження злочинності та кримінального правосуддя питання протидії злочинам у сфері інформаційних технологій передбачені у пункті «Міжнародне співробітництво та технічна допомога у запобіганні всім формам злочинності та боротьбі з ними» у контексті сучасних тенденцій в галузі злочинності, зокрема використання сучасних технологій як засобу вчинення злочинів та інструменту боротьби зі злочинністю.

Як зазначає учасник Конгресу ООН з попередження злочинності та кримінального правосуддя В.О. Туляков, звертаючи увагу до прояву нових форм злочинності, Сторони домовились розвивати співробітництво для боротьби з комп'ютерною злочинністю, товарною контрабандою, погрозами, пов'язаними з технічними досягненнями та зміною методів незаконного виготовлення та обігу вогнепальної зброї, її складових частин і компонентів [9].

На Конгресі ООН були розглянуті загрози використання інформаційних технологій з метою торгівлі людьми та організації незаконної міграції, проблеми пов'язані із злочинним використанням віртуальних активів, онлайн-ринків незаконного обігу наркотиків, дитячої порнографії та зброї.

В ООН сформувався інституційний механізм протидії злочинам, що охоплює різні формати співробітництва держав у досліджуваній галузі. Відмінна риса інституційного механізму ООН з протидії злочинам полягають у тому, що робота зосереджена на ініціативах з розробки міжнародно-правових засад, стратегічних напрямів та концепцій протидії злочинам у сфері інформаційних технологій та планів роботи з реалізації.

На думку С.В. Копійки, модернізація політики міжнародних організацій щодо інформаційної безпеки визначається їх можливостями забезпечити багатосторонній діалог міжнародних акторів, врахувати різні позиції суб'єктів глобального управління з протидії новітнім інформаційним загрозам та виступати згідно зі статутними повноваженнями як універсальні міжнародні платформи для формування консенсусу у вирішенні актуальних безпекових проблем [10, с. 107].

Т.І. Алексеева зазначає, що сучасні пріоритети ООН спрямовані на координацію зусиль щодо забезпечення комплексного підходу до розв'язання міжнародних проблем, у тому числі вирішення проблем у напрямі безпеки у сфері міжнародної інформації [11, с. 9].

Дослідження доповідей про результати діяльності спеціалізованих структур ООН із протидії злочинам у сфері інформаційних технологій дозволило визначити практичні заходи: створення контактних центрів для реалізації співробітництва держав щодо протидії злочинам у сфері інформаційних технологій; розробка механізмів проведення двосторонніх, регіональних і багатосторонніх консультацій; зміцнення довіри регіональних та багатосторонніх форумів; створення міжнародної бази даних з кращими практиками з розвитку національного законодавства та вдосконалення стратегій у розглянутій сфері; створення додаткових механізмів для розгляду запитів правової допомоги у кримінальних справах про злочини у сфері інформаційних технологій; розвиток можливостей проведення цифрових експертиз.

Висновки. Функціонування інституційного механізму ООН щодо протидії злочинам у сфері інформаційних технологій здійснюється з урахуванням тенденцій: зростаюча необхідність реалізації ефективної міжнародної співпраці; збільшення ролі нормативно-правових засад міждержавної взаємодії та можливостей правоохоронних органів; взаємопов'язаність інформаційних злочинів із транснаціональною організованою злочинністю; потреба у відповідності положень щодо криміналізації, процесуальних повноважень правоохоронних органів, визначення юрисдикції та отримання цифрових доказів; підвищення актуальності оперативного реагування на запити взаємної правової допомоги; активізація розробки практичних заходів з мінімізації загроз для дітей, які виникають у сфері інформаційних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Резолюції Генеральної Асамблеї 53/70 від 4 грудня 1998 року «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки». URL. <https://www.un.org/ru/ga/53/docs/53res1.shtml>.
2. Попко В.В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського Національного Університету, серія право*. 2021. Випуск 66. С. 276–283.
3. Глобальна контртерористична стратегія ООН. 03.08.2021. URL. https://www.wiki-data.uk-ua.nina.az/%D0%9E%D0%9D.html#cite_note-7.
4. Salvador Declaration Calls for Criminal Justice Reform to Safeguard Human Rights, Security and Development. URL. <http://www.un.org/en/conf/crimecongress2010/pdf/pr100419-1.pdf>.
5. Резолюції Генеральної Асамблеї ООН 74/247 від 27 грудня 2019 року «Протидія використанню інформаційно-комунікаційних технологій у злочинних цілях». URL. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/31/PDF/N1944031.pdf?OpenElement>.
6. Семко М.О. Нормотворча діяльність ООН щодо забезпечення інформаційної безпеки у війсьній сфері. *Юридичний науковий електронний журнал*. 2022. № 8. С. 580–583.
7. Захист дітей у цифровому середовищі: рекомендації для індустрій. Міжнародний союз електрозв'язку. Женева: Shutterstock, 2020. 79 с.
8. Керівництво з оцінки національних спроможностей. Грудень 2020. Європейське агентство з питань мережевої та інформаційної безпеки. ENISA. 2020. 83 с.

9. Шляхи Кіото: XIV-й конгрес ООН з попередження злочинності та кримінального правосуддя та перспективні завдання сучасної кримінології. 22.04.2021. Lexinform. URL. <https://lexinform.com.ua/podii/shlyahy-kioto-xiv-j-kongres-oon-z-poperedzhennya-zlochynnosti-ta-kryminalnogo-pravosuddya-ta-perspektyvni-zavdannya-suchasnoyi-kryminologiyi/>.
10. Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя*. 2020. № 1. С. 102–109.
11. Алексеева Т.І. Міжнародні організації: сучасні пріоритети та нові виклики в системі міжнародної інформаційної безпеки. *Науковий вісник Ужгородського національного університету. Серія: міжнародні економічні відносини та світове господарство*. 2020. Випуск 34. С. 9–12.