Кримінальне право та кримінологія

УДК 343.533:341.48

DOI https://doi.org/10.5281/zenodo.18402814

Механізми протидії інформаційним злочинам у цифрову епоху на рівні міжнародного права

Кожушко Олена Олегівна,
кандидат юридичних наук, доцент кафедри правових та інформаційних технологій, Відокремлений структурний підрозділ закладу вищої освіти «Відкритий міжнародний університет розвитку людини «Україна» Хмельницький інститут соціальних технологій, м. Хмельницький, Україна, https://orcid.org/0000-0001-6939-1466

Товпига Ліна Миколаївна,
доктор філософії в галузі права, доцент кафедри господарського, повітряного та космічного права, Національний авіаційний університет, Київ, Україна, https://orcid.org/0000-0003-0625-1188

Бабіна Валентина Олександрівна,
кандидат політичних наук, доцент кафедри міжнародних відносин та права, Інститут гуманітарних наук, Національний університет «Одеська політехніка», м. Одеса, Україна, https://orcid.org/0000-0003-2796-5024

Прийнято: 11.01.2026 | Опубліковано: 28.01.2026

Анотація. Мета дослідження полягає у комплексному аналізі механізмів протидії інформаційним злочинам у цифрову епоху на рівні

міжнародного права з урахуванням сучасних безпекових викликів, зумовлених гібридними конфліктами, транснаціональною кіберзлочинністю та використанням інформаційного простору як інструменту політичного впливу. Особливу увагу приділено міжнародно-правовим засобам реагування на інформаційні злочини в умовах збройних конфліктів та тимчасової окупації територій, зокрема їхнього впливу на забезпечення міжнародної стабільності та правопорядку. Методи дослідження охоплюють формально-юридичний, порівняльно-правовий, системно-структурний та аналітичний методи, що дає змогу оцінити ефективність чинних міжнародних норм і практик у сфері протидії інформаційним злочинам. Водночас у роботі застосовано елементи контент-аналізу міжнародних документів і сучасних наукових публікацій з метою виявлення домінантних підходів та тенденцій правового регулювання. Результати дослідження засвідчують, що міжнародно-правові механізми протидії інформаційним злочинам формуються як багаторівнева система, що охоплює криміналізацію відповідних діянь, міжнародну правову допомогу, стандарти захисту прав людини та інструменти колективної безпеки. Виявлено, що в умовах гібридної агресії інформаційні злочини використовуються як компонент політики експансіонізму, що підтверджується аналізом практик на тимчасово окупованих територіях України. Відповідно, чинні міжнародні механізми залишаються фрагментованими та потребують подальшого вдосконалення і систематизації. Обґрунтовано необхідність посилення універсальних міжнародно-правових інструментів протидії інформаційним злочинам, зокрема шляхом удосконалення процедур обміну електронними доказами, розширення міжнародної координації та інтеграції безпекових і правозахисних методик. Отримані результати можуть бути використані для розвитку національних стратегій інформаційної безпеки, удосконалення правозастосовної практики та подальших наукових досліджень у сфері міжнародного інформаційного права.

 ISSN: 3041-2110

Ключові слова: міжнародні відносини, міжнародна відповідальність, гібридні загрози, інформаційний простір, кібербезпека, національна безпека, цифрова епоха, політичні процеси, правове регулювання, міжнародна правова допомога.

Mechanisms for counteracting information crimes in the digital era under international law

Olena Kozhushko,
Candidate of Juridical Sciences, Associate Professor, Separate Structural Subdivision of Higher Education Institution Open International University of Human Development «Ukraine» Khmelnytskyi Institute of Social Technologies, Khmelnytskyi, Ukraine, https://orcid.org/0000-0001-6939-1466

Lina Tovpyha,
PhD in Law, Docent of the Department of Commercial, Air and Space Law, National Aviation University, Kyiv, Ukraine, https://orcid.org/0000-0003-0625-1188

Valentyna Babina,
Candidate of Political Sciences, Associate Professor, Department of International Relations and Law, Institute of Humanities, National University «Odessa Polytechnic», Odesa, Ukraine, https://orcid.org/0000-0003-2796-5024

Abstract. The purpose of this study is to provide a comprehensive analysis of mechanisms for counteracting information crimes in the digital era at the international law level, taking into account contemporary security challenges posed by hybrid conflicts, transnational cybercrime, and the use of the information space

as an instrument of political influence. Particular attention is paid to international legal instruments for responding to information crimes in situations of armed conflict and temporary occupation of territories, as well as to their impact on the maintenance of international stability and legal order. The research employs formal legal, comparative legal, systemic-structural, and analytical methods, enabling it to assess the effectiveness of existing international norms and practices in counteracting information crimes. In addition, elements of content analysis of international legal instruments and contemporary academic publications are applied in order to identify dominant regulatory approaches and prevailing trends in legal governance. The findings indicate that international legal mechanisms for counteracting information crimes are developing as a multi-level system that includes the criminalisation of relevant acts, international legal assistance, human rights protection standards, and collective security instruments. It is established that under conditions of hybrid aggression, information crimes are used as an integral component of expansionist policy, which is confirmed by the analysis of practices implemented in the temporarily occupied territories of Ukraine. At the same time, existing international mechanisms remain fragmented and require further harmonisation and systematisation. The study substantiates the need to strengthen universal international legal instruments to counter information crimes, in particular by improving procedures for the exchange of electronic evidence, expanding international coordination, and integrating security-oriented and human rights-based approaches. The results obtained may be used to develop national information security strategies, improve law enforcement practices, and support further academic research in international information law.

Keywords: international relations, international responsibility, hybrid threats, information space, cybersecurity, national security, digital age, political processes, legal regulation, international legal assistance.

Постановка проблеми. Глобалізація інформаційного простору та стрімкий розвиток цифрових технологій зумовили трансформацію

традиційних форм злочинності та появу якісно нових загроз, що отримали узагальнену назву «інформаційні злочини». Такі діяння часто вчиняються поза межами національних юрисдикцій, характеризуються високим рівнем латентності та використовуються не лише кримінальними угрупованнями, а й державними та квазідержавними установами під час гібридних конфліктів.

Актуалізація проблеми протидії інформаційним злочинам набуває особливого значення у контексті міжнародної безпеки та захисту прав людини. Використання дезінформації, кібератак і маніпулятивних цифрових практик у поєднанні з політикою експансіонізму створює загрозу суверенітету держав і стабільності міжнародного правопорядку. Такі дії на тимчасово окупованих територіях України демонструють, що інформаційні злочини можуть бути інтегровані в систему управління та контролю населення, що виходить за межі класичних уявлень про кіберзлочинність як суто кримінально-правову проблему.

Зв’язок зазначеної проблематики з важливими науковими та практичними завданнями полягає у необхідності розроблення ефективних міжнародно-правових механізмів, здатних забезпечити своєчасне реагування на інформаційні злочини, належну міжнародну координацію та дотримання стандартів прав людини. Це зумовлює потребу в системному аналізі чинних міжнародних інструментів і пошуку шляхів їхнього удосконалення.

Аналіз останніх досліджень і публікацій. Протягом останніх п’яти років проблема інформаційних злочинів та міжнародно-правових механізмів їхній протидії є предметом активних наукових досліджень у галузях міжнародного права, безпекових блоках та інформаційної політики. Зокрема, дослідники М. Шмітт та А. Паккам (M. Schmitt & A. Pakkam) [1] підкреслюють, що традиційні правові інструменти виявляються недостатніми для реагування на транснаціональні цифрові загрози, які поєднують елементи кіберзлочинності, інформаційних операцій і політичного впливу.

Численні новітні публікації присвячено застосуванню норм міжнародного публічного права до кібер- та інформаційних операцій. Аналізуючи практики держав, автор С. Гаатая (S. Haataja) [2] засвідчує, що відсутність узгоджених універсальних стандартів реагування створює правову невизначеність та сприяє використанню інформаційних злочинів як інструменту непрямого тиску у міждержавних відносинах.

Окремий напрям сучасних досліджень пов'язаний із міжнародною відповідальністю держав та допустимими заходами реагування у відповідь на інформаційні злочини. Так, вчений С. Гаатая (S. Haataja) [3] обґрунтовує, що застосування контрзаходів у кіберпросторі має здійснюватися з урахуванням принципів необхідності та пропорційності, що істотно обмежує свободу дій держав і ускладнює міжнародну координацію.

Важливе місце у сучасному науковому дискурсі посідають дослідження некінетичних наслідків кібероперацій у контексті міжнародного гуманітарного права. У межах цього аналізу науковець Ґ. Бігґіо (G. Biggio) [4] наголошує, що порушення функціональності інформаційних систем або критичної інфраструктури може мати суттєві гуманітарні наслідки навіть за відсутності фізичних руйнувань, що вимагає переосмислення традиційних методів оцінювання шкоди.

Окрему групу становлять дослідження впливу інформаційних злочинів на права людини. Відповідно до цього транснаціональний характер цифрових операцій, здатний призводити до екстратериторіальних порушень права на приватність, свободи вираження поглядів і доступу до інформації, розглядає автор М. Міланович (M. Milanovic) [5]. Акцентовано на необхідності інтеграції стандартів міжнародного права, прав людини у механізми протидії інформаційним злочинам.

Одночасно у науковій літературі простежується зростання інтересу до нормативного та політичного виміру інформаційних злочинів. Дослідник Б. Маднік зі співавторами (B. Madnick et al.) [6] аналізують роль міжнародних

 ISSN: 3041-2110

норм і неформальних режимів управління кіберпростором у стримуванні деструктивної поведінки держав та підтриманні стабільності міжнародного правопорядку.

Крім того, значний науковий інтерес становлять дослідження, присвячені гібридному характеру інформаційних злочинів у контексті збройних конфліктів. Так, науковець П. Лисянський [7] аналізує діяльність профспілкових організацій Російської Федерації на тимчасово окупованих територіях України як інструмент посилення експансіоністської політики. Емпірично доведено, що формально легальні структури можуть використовуватися для здійснення інформаційного та політичного впливу, що має ознаки системних інформаційних правопорушень і потребує міжнародно-правового оцінювання.

Питання експансіонізму Російської Федерації на тимчасово непідконтрольних частинах Луганської та Донецької областей у 2014–2022 роках вивчає дослідник П. Лисянський [8]. Зокрема, розглянуто інформаційні впливи як основний елемент стратегії контролю над окупованими територіями. Таким чином, у наведених роботах практично обґрунтовано значущість аналізу інформаційних злочинів у ширшому міжнародно-правовому контексті.

Виділення невирішених раніше частин загальної проблеми. Попри помітне зростання кількості наукових публікацій, присвячених кіберзлочинності, інформаційній безпеці та правовому регулюванню цифрового простору, у сучасному науковому дискурсі й надалі зберігається низка суттєвих нерозв’язаних питань. Саме ці аспекти ускладнюють формування цілісного й ефективного міжнародно-правового механізму протидії інформаційним злочинам у цифрову епоху.

Передусім проблемним залишається питання міжнародно-правової кваліфікації інформаційних злочинів у контексті гібридних конфліктів. Чинні міжнародні договори та універсальні конвенційні підходи здебільшого

 ISSN: 3041-2110

орієнтовані на класичні прояви кіберзлочинності, зокрема незаконний доступ до інформаційних систем, втручання в їхню роботу або шахрайство з використанням комп'ютерних технологій. Водночас системні інформаційні впливи, масштабні дезінформаційні кампанії та використання формально цивільних інституцій як каналів інформаційної агресії часто залишаються поза межами чіткої міжнародно-правової регламентації та усталеної практики правового оцінювання.

Ще однією актуальною проблемою є відсутність узгодженої концептуальної моделі міжнародної відповідальності за інформаційні злочини, що здійснюються за участю держав або за їхньої мовчазної згоди. У наукових дослідженнях переважають або кримінально-правові підходи, зосереджені на індивідуальній відповідальності, або доктринальні тлумачення норм міжнародного публічного права, які не завжди узгоджуються між собою. Це ускладнює практичне застосування механізмів міжнародної відповідальності у випадках системних інформаційних правопорушень.

На окрему увагу заслуговує і збереження дисбалансу між безпековими механізмами реагування та міжнародними правозахисними стандартами. На практиці це проявляється у складнощах, пов'язаних із доступом до електронних доказів, обміном інформацією між державами та забезпеченням належного рівня захисту персональних даних. Причинами такого стану є різний рівень цифрової спроможності держав, відмінності у правових системах та політичні обмеження міжнародного співробітництва.

Отже, ці проблеми мають принципове значення для розуміння природи інформаційних злочинів у цифрову епоху та обґрунтовують потребу у ґрунтовному міжнародно-правовому аналізі, що поєднує кримінально-правові, безпекові та правозахисні практики.

Формулювання мети та завдань статті. Метою роботи є комплексне дослідження механізмів протидії інформаційним злочинам у цифрову епоху

на рівні міжнародного права з урахуванням сучасних викликів, пов'язаних із гібридними конфліктами та транснаціональною інформаційною агресією.

Для досягнення мети дослідження передбачено розв'язання таких основних завдань:

1) проаналізувати стан та особливості міжнародно-правового регулювання протидії інформаційним злочинам у контексті сучасних безпекових викликів;

2) узагальнити наукові підходи до розуміння інформаційних злочинів як складника гібридних загроз та визначити проблеми міжнародної відповідальності за такі діяння;

3) окреслити основні напрями вдосконалення міжнародно-правових механізмів протидії інформаційним злочинам з урахуванням необхідності поєднання безпекових заходів і стандартів захисту прав людини.

Виклад основного матеріалу дослідження. Сучасна система міжнародно-правового регулювання протидії інформаційним злочинам формується на основі поєднання договірних норм, універсальних та регіональних стандартів, політико-правових інструментів «м'якого права». Центральне місце серед обов'язкових міжнародних актів посідає Будапештська Конвенція Ради Європи про кіберзлочинність 2001 року, яка визначає базові засади криміналізації правопорушень у сфері використання інформаційних технологій, уніфікації процесуальних механізмів та міжнародної правової допомоги у збиранні й обміні електронними доказами. Наразі цей документ залишається основним орієнтиром для гармонізації національних законодавств у сфері боротьби з кіберзлочинністю [9].

Важливе значення для міжнародного регулювання має Додатковий протокол до Будапештської конвенції, спрямований на криміналізацію поширення расистських і ксенофобських матеріалів у цифровому середовищі. Положення цього документа демонструють поступовий перехід від суто

 ISSN: 3041-2110

технічного розуміння кіберзлочинності до врахування контентних і соціально небезпечних форм інформаційних правопорушень [10].

Водночас новим етапом розвитку міжнародно-правових механізмів було ухвалення у 2024 році проєкту Конвенції ООН проти кіберзлочинності, яка має на меті створення глобальної рамки співробітництва держав у цій сфері. На відміну від регіональних інструментів, Конвенція орієнтована на забезпечення універсальності стандартів криміналізації та міжнародної взаємодії, що особливо актуально з огляду на транснаціональний характер інформаційних злочинів [11].

Окрему групу правових орієнтирів становлять норми відповідальної поведінки держав у кіберпросторі, розроблені в межах Організації Об'єднаних Націй, які, хоча й не мають обов'язкової юридичної сили, є значущими у формуванні практики застосування міжнародного права до інформаційних та кібероперацій, зокрема щодо принципів суверенітету, невтручання та належної обачності.

Крім того, значний вплив на міжнародні підходи до протидії інформаційним злочинам справляють регіональні акти, зокрема директиви Європейського Союзу у сфері безпеки мереж і інформаційних систем (NIS та NIS2) [12]. Вони формують стандарти захисту критичної цифрової інфраструктури та опосередковано визначають напрям розвитку національних політик інформаційної безпеки в державах, які орієнтуються на європейські правові моделі.

Загалом зазначені нормативні акти засвідчують фрагментований, але поступово інституціоналізований характер міжнародно-правового регулювання у сфері протидії інформаційним злочинам, що зумовлює потребу подальшої координації та систематизації правових підходів на глобальному рівні.

У сучасних умовах інформаційні злочини дедалі частіше є не лише ізольованими кримінальними правопорушеннями, а й елементом стратегій

 ISSN: 3041-2110

гібридної агресії. Йдеться про системні інформаційні впливи, спрямовані на маніпулювання громадською думкою, дестабілізацію політичних процесів, підрив довіри до державних інституцій та формування контрольованого інформаційного середовища [13, p. 39–42].

Згідно з цим актуальна міжнародно-правова доктрина розглядає інформаційні злочини як багатовимірне явище, що поєднує елементи кіберзлочинності, інформаційних операцій і політико-правового впливу. У новітніх дослідженнях підкреслюється, що такі діяння не можуть бути адекватно схарактеризовані виключно в межах національного кримінального права, оскільки вони безпосередньо зачіпають питання суверенітету, міжнародної стабільності та колективної безпеки. Це зумовлює необхідність виходу за межі традиційного кримінально-правового аналізу та врахування норм міжнародного публічного права, зокрема принципів невтручання, відповідальності держав і підтримання міжнародного миру та безпеки [14, p. 58–60].

У цьому контексті однією з ключових проблем міжнародно-правової протидії інформаційним злочинам є визначення меж допустимого реагування держав на інформаційні та кібероперації. В останніх дослідженнях наголошено, що більшість таких дій не досягають класичного порогу застосування сили у розумінні міжнародного публічного права, водночас можуть мати кумулятивний характер і поступово спричиняти суттєві безпекові ризики для держави-жертви [15, p. 368]. Зокрема, наголошено на серії взаємопов’язаних інформаційних або кібероперацій, здатних впливати на стратегічну стабільність, політичні процеси та довіру до державних інститутів, навіть за відсутності відкритої збройної агресії. Така «підпорогова» динаміка ускладнює правову кваліфікацію відповідних дій і створює простір для маневру з боку держав, які прагнуть уникнути міжнародно-правової відповідальності.

Ще одним значущим аспектом під час збройних конфліктів є проблема некінетичних наслідків інформаційних операцій. Порушення функціональності інформаційних систем або критичної інфраструктури може мати серйозні гуманітарні наслідки навіть за відсутності фізичних руйнувань, що вимагає переосмислення традиційних практик оцінювання шкоди у міжнародному гуманітарному праві [4, p. 241]. Отже, йдеться про ситуації, коли інформаційні або кібероперації призводять до тривалого припинення роботи систем охорони здоров'я, енергопостачання, водозабезпечення чи зв'язку, що безпосередньо впливає на захист цивільного населення та реалізацію основоположних прав людини.

У сучасних дослідженнях зазначено, що зосередження виключно на фізичних наслідках атак не відображає реального масштабу шкоди, заподіяної в цифровому середовищі. Некінетичні ефекти можуть мати кумулятивний характер, поступово підриваючи життєздатність цивільної інфраструктури та здатність держави виконувати базові функції. Це актуалізує питання застосування принципів військової необхідності, пропорційності та розрізнення у випадках, коли шкоду заподіяно не у формі матеріальних руйнувань, а через втрату або деградацію функціональності об'єктів.

Таким чином, інформаційні операції у збройних конфліктах потребують оцінювання не лише з погляду засобів і методів ведення війни, а й з урахуванням їхнього фактичного впливу на цивільне населення та гуманітарну ситуацію загалом. Це створює додаткові виклики для міжнародного права та спричиняє необхідність розвитку гнучкіших критеріїв правової кваліфікації шкоди, завданої внаслідок некінетичних дій.

Додатковою глобальною проблемою у сучасних міжнародно-правових дискусіях є питання цифрового суверенітету. Держави дедалі активніше намагаються встановити контроль над національним інформаційним простором, обґрунтовуючи це необхідністю захисту від зовнішніх інформаційних загроз, втручання у внутрішні справи та деструктивних

 ISSN: 3041-2110

інформаційних впливів. Водночас такі заходи нерідко призводять до запровадження обмежень на транскордонний обіг інформації, посилення державного контролю над цифровою інфраструктурою та діяльністю приватних суб'єктів, що породжує конфлікти з міжнародними зобов'язаннями у сфері свободи вираження поглядів, доступу до інформації та захисту приватності [16].

З огляду на це визначено, що прагнення до цифрового суверенітету не є однорідним явищем і може реалізовуватися як у формі легітимних заходів кібербезпеки, так і через надмірний захист інформаційного простору. В іншому випадку цифровий суверенітет перетворюється на інструмент обмеження демократичних свобод і фрагментації глобального інформаційного середовища, що ускладнює міжнародну співпрацю та створює додаткові можливості для зловживань у сфері інформаційної політики.

На цьому тлі міжнародно-правові механізми протидії інформаційним злочинам мають враховувати необхідність досягнення балансу між суверенним правом держав на захист власного інформаційного простору та зобов'язаннями щодо дотримання міжнародних стандартів прав людини. Відсутність такого балансу підвищує ризик діяльності, спрямованої на запобігання інформаційним загрозам, що може набути ознак правопорушень у сфері свободи інформації та цифрових прав.

Окремий вимір проблеми становить вплив інформаційних злочинів на демократичні інститути та суспільні процеси. Поширення дезінформації, маніпулятивного контенту та координованих інформаційних кампаній безпосередньо підриває довіру до демократичних процедур, зокрема виборчих процесів, діяльності органів публічної влади та незалежних медіа. Такі практики сприяють поляризації суспільства, зниженню легітимності демократичних інститутів і формуванню передумов для політичної дестабілізації. Зокрема, наголошено, що інформаційні злочини у цифровому середовищі здатні системно впливати на процеси ухвалення політичних

рішень і громадську участь, створюючи загрозу функціонуванню демократичних режимів навіть за відсутності прямого фізичного втручання [17].

Досвід України переконливо засвідчує, що на тимчасово окупованих територіях інформаційні злочини не мають ізольованого характеру, а реалізуються як частина комплексної системи гібридного впливу. У таких умовах інформаційні правопорушення тісно поєднуються з діяльністю формально цивільних організацій (псевдопрофспілкових, культурних, освітніх та громадських структур), які виконують функції трансляції пропагандистських наративів, легітимації окупаційної адміністрації та здійснення соціального контролю над населенням. Ці організації використовуються як інструменти інституціоналізації інформаційного впливу, що дає змогу приховувати системні інформаційні злочини під виглядом законної суспільної діяльності [7, с. 53–55].

Особливістю таких практик є їхня довготривалість і системність, що виходить за межі окремих актів дезінформації або маніпулятивного контенту. Інформаційні злочини на окупованих територіях функціонують як елемент цілісної стратегії контролю над інформаційним простором, спрямованої на формування лояльної ідентичності, придушення альтернативних джерел інформації та викривлення уявлень про правовий статус територій і легітимність державної влади. У цьому сенсі вони набувають ознак системних інформаційних правопорушень міжнародного характеру, що потребують не лише кримінально-правового, а й міжнародно-правового оцінювання [8, с. 101].

Ці методи створюють додаткові виклики для міжнародного права, оскільки традиційні правові механізми протидії переважно орієнтовані на класичні форми агресії або індивідуальну кримінальну відповідальність (табл. 1). Натомість використання формально цивільних структур як носіїв інформаційних злочинів ускладнює ідентифікацію суб’єктів відповідальності,

 ISSN: 3041-2110

доведення ефективного контролю та застосування міжнародно-правових механізмів реагування. Це сприяє розвитку підходів, які б забезпечували врахування інституційної та системної природи інформаційних злочинів у контексті збройних конфліктів і тимчасової окупації.

Таблиця 1

Проблеми протидії інформаційним злочинам

Проблеми	Шляхи розв'язання	Перспективи розвитку
Транснаціональний характер інформаційних злочинів	Уніфікація міжнародних кримінально-правових норм	Формування універсальних стандартів відповідальності
Порушення права на приватність	Запровадження чітких процедур доступу до електронних доказів	Підвищення рівня довіри до міжнародної співпраці
Зловживання заходами інформаційної безпеки	Судовий та міжнародний контроль	Інтеграція правозахисних практик у безпекову політику

Джерело: власна розробка авторів

У таблиці узагальнено основні виклики, що постають перед міжнародним правом у сфері протидії інформаційним злочинам, та продемонстровано взаємозв'язок між безпековими заходами й правозахисними стандартами. Показано, що ефективність міжнародно-правових механізмів безпосередньо залежить від здатності держав поєднувати кримінально-правові інструменти з інституційними гарантіями захисту прав людини. Зокрема, уніфікація кримінально-правових норм без належного процесуального забезпечення може призвести до зростання кількості конфліктів юрисдикцій та зловживань. Водночас розроблення універсальних стандартів доступу до електронних доказів створює передумови для підвищення ефективності міжнародної співпраці та зміцнення довіри між державами.

Ще одним значущим виміром міжнародно-правових механізмів протидії інформаційним злочинам є інституційна взаємодія між державами та

міжнародними організаціями. Її значення зростає в умовах, коли інформаційні злочини виходять за межі юрисдикції однієї держави та мають системний характер. Інституційні механізми покликані компенсувати обмеження договірного права шляхом оперативного обміну інформацією, аналітичної підтримки та координації спільних дій.

У сучасній практиці такі механізми функціонують на основі принципів добровільної участі, взаємної довіри та дотримання міжнародних стандартів прав людини. Відповідно, їхня ефективність нерідко знижується через асиметрію інформації, різний рівень технічної спроможності держав і політичні обмеження співпраці. Особливо гостро ці проблеми проявляються у випадках, коли інформаційні злочини є частиною державної або квазідержавної стратегії впливу.

Зокрема, досвід протидії інформаційній агресії на тимчасово окупованих територіях України засвідчує, що відсутність оперативних міжнародних механізмів реагування сприяє інституціалізації інформаційних правопорушень та їхній легітимації у псевдоправових формах. Це підкреслює необхідність переходу від фрагментарних інституційних рішень до системної міжнародної координації.

Узагальнюючи, на рис. 1 відображено багатовимірний характер міжнародної політики протидії інформаційним злочинам. Кожен із зазначених елементів виконує самостійну функцію, водночас перебуваючи у тісному взаємозв’язку з іншими компонентами. Так, криміналізація інформаційних злочинів без ефективних механізмів міжнародної правової допомоги не забезпечує реального притягнення винних до відповідальності. Аналогічно,

ISSN: 3041-2110

інституційна координація втрачає практичну цінність без чітких правових рамок та процедур захисту прав людини.

Рис. 1. Основні аспекти міжнародної політики протидії інформаційним злочинам

Джерело: власна розробка авторів

Наведені дані дають змогу зробити висновок, що міжнародно-правова протидія інформаційним злочинам повинна розглядатися як цілісна система, у якій превентивні заходи та підвищення інформаційної стійкості відіграють не менш важливу роль, ніж репресивні інструменти кримінального права. Така практика відповідає сучасним тенденціям розвитку міжнародного права безпеки та сприяє адаптації правових механізмів до динаміки цифрового середовища.

Проведений аналіз засвідчує, що чинні міжнародно-правові механізми протидії інформаційним злочинам характеризуються обмеженою універсальністю та значною залежністю від політичних і інституційних чинників. Наявні інструменти здебільшого спрямовані на реагування на окремі прояви кіберзлочинності, тоді як системні інформаційні злочини, пов’язані з гібридною агресією, залишаються недостатньо врегульованими.

 ISSN: 3041-2110

Одночасно емпіричні узагальнення демонструють, що поєднання кримінально-правових, інституційних і правозахисних практик створює передумови для формування ефективнішої моделі міжнародної протидії інформаційним злочинам. Особливої значущості набуває інтеграція досвіду держав, які безпосередньо стикаються з інформаційною агресією, у процес розроблення міжнародних стандартів.

Висновки. У процесі дослідження продемонстровано, що інформаційні злочини у цифрову епоху не є виключно проблемою кримінального права, а трансформувалися у складний багатовимірний феномен, який безпосередньо впливає на міжнародну безпеку, суверенітет держав і реалізацію прав людини. У сучасних умовах вони дедалі частіше використовуються як інструмент гібридної агресії, поєднуючись з політичними, економічними та соціальними механізмами впливу.

Аналіз міжнародно-правових механізмів протидії інформаційним злочинам показав, що наявна система регулювання має фрагментований характер і не забезпечує належної реакції на системні інформаційні правопорушення, пов’язані з експансіоністською політикою та збройними конфліктами. Крім того, міжнародні договори та інституційні платформи переважно зосереджені на технічних аспектах кіберзлочинності, залишаючи поза увагою комплексний характер інформаційної агресії.

У роботі обґрунтовано, що ефективна міжнародно-правова протидія інформаційним злочинам можлива лише за умови інтеграції кримінально-правових, інституційних та правозахисних практик. Особливого значення набуває гармонізація процедур міжнародної правової допомоги, удосконалення механізмів доступу до електронних доказів і посилення інституційної координації між державами. Водночас боротьба з інформаційними злочинами не повинна призводити до звуження змісту та обсягу фундаментальних прав і свобод людини.

ISSN: 3041-2110

Подальші наукові розвідки доцільно зосередити на розробленні універсальних критеріїв міжнародної відповідальності за інформаційні злочини у контексті гібридних конфліктів, зокрема на вдосконаленні моделей взаємодії між безпековими та правозахисними інститутами у цифровому середовищі.

Список використаних джерел

1. Schmitt M. N., Pakkam A. S. Cyberspace and the *jus ad bellum*: the state of play. *International Law Studies*. 2024. Vol. 103. P. 193–229. URL: https://digital-commons.usnwc.edu/ils/vol103/iss1/7/.

2. Haataja S. Cyber operations and automatic hack backs under international law on necessity. *Computer Law & Security Review*. 2024. Vol. 53. Art. 105992. DOI: https://doi.org/10.1016/j.clsr.2024.105992.

3. Haataja S. Cyber operations and collective countermeasures under international law. *Journal of Conflict & Security Law*. 2020. Vol. 25, № 1. P. 33–51. DOI: https://doi.org/10.1093/jcsl/kraa003.

4. Biggio G. Regulating non-kinetic effects of cyber operations: the «loss of functionality» approach and the military necessity–humanity balance under international humanitarian law. *Journal of Conflict & Security Law*. 2025. Vol. 30, № 2. P. 241–263. DOI: https://doi.org/10.1093/jcsl/kraf008.

5. Milanovic M. Surveillance and cyber operations. The Routledge handbook on extraterritorial human rights obligations / eds M. Milanovic, S. Skogly, A. Benvenisti. London, New York: Routledge, 2021. P. 366–379. DOI: https://doi.org/10.4324/9781003090014-33.

6. Madnick B., Huang K., Madnick S. The evolution of global cybersecurity norms in the digital age: a longitudinal study of the cybersecurity norm development process. *Information Security Journal: A Global Perspective*. 2024. Vol. 33, № 3. P. 204–225. DOI: https://doi.org/10.1080/19393555.2023.2201482.

7. Лисянський П. Діяльність профспілкових організацій РФ на тимчасово окупованих територіях України як інструмент посилення політики експансіонізму. *Наукові праці МАУП*. 2024. № 3 (75). С. 51–57. DOI: https://doi.org/10.32689/2523-4625-2024-3(75)-8.

8. Лисянський П. Л. Експансіонізм РФ на тимчасово непідконтрольних частинах територій Луганської та Донецької областей у 2014–2022 роках. *Вісник НТУУ КПІ. Політологія. Соціологія. Право*. 2024. № 4 (64). С. 101–108. DOI: https://doi.org/10.20535/2308-5053.2024.4(64).322710.

9. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. *Cybercrim*e. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата звернення: 20.11.2025).

10. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189). *Council of Europe*. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 (дата звернення: 20.11.2025).

11. United Nations Convention against cybercrime; strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes. New York: UNODC, 2024. URL: https://www.unodc.org/documents/newyork/Documents/01_UN_Convention_against_Cybercrime_-_OEWG_VN.pdf (дата звернення: 20.11.2025).

12. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 december 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *European Union*. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 20.11.2025).

13. Devanny J., Goldoni L. R. F., Medeiros B. Strategy in an uncertain domain: threat and response in cyberspace. *Journal of Strategic Security*. 2022. Vol. 15, № 2. P. 34–47. DOI: https://doi.org/10.5038/1944-0472.15.2.1954.

14. Chatinakrob T. Interplay of international law and cyberspace: state sovereignty violation, extraterritorial effects, and the paradigm of cyber sovereignty. *Chinese Journal of International Law*. 2024. Vol. 23, № 1. P. 25–72. DOI: https://doi.org/10.1093/chinesejil/jmae005.

15. Hung H. T. (Bosco). Multilateral cooperation in building critical infrastructure security and resilience: case of American deterrence of Chinese cyberthreats. *Journal of Cyber Policy*. 2024. Vol. 9, № 3. P. 351–376. DOI: https://doi.org/10.1080/23738871.2024.2443421.

16. DeNardis L. The internet in everything: freedom and security in a world with no off switch. New Haven, CT: Yale University Press, 2020. 256 p. DOI: https://doi.org/10.12987/yale/9780300233070.001.0001.

17. Shawe R. Cybersecurity and human rights: navigating the balance between security and freedom in the digital era. *Journal of Information Technology and Integrity*. 2025. Vol. 3, № 2. Art. 110. DOI: https://doi.org/10.33790/jiti1100110.

 ISSN: 3041-2110