МІЖНАРОДНО-ПРАВОВІ АСПЕКТИ ЗАХИСТУ ПРАВ ЛЮДИНИ В УМОВАХ КІБЕРЗАГРОЗ

КОЦЮРУБА Сергій Ілліч - аспірант кафедри міжнародного та європейського права Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут»

ORCID: 0009-0006-1741-4308

УДК 41.67:343.9:004.9

DOI: https://doi.org/10.71404/NP.2025.1.61

У сучасному світі кіберзагрози стали одними з ключових викликів для забезпечення прав людини, оскільки вони охоплюють широкий спектр ризиків, включаючи незаконне збирання та використання персональних даних, маніпулювання інформацією, кібератаки на критичну інфраструктуру та порушення свободи вираження поглядів. В умовах цифрової трансформації суспільства постає необхідність удосконалення міжнародно-правових механізмів для забезпечення прав людини в кіберпросторі. Це зумовлено як швидким розвитком технологій, так і зростаючою кількістю кіберінцидентів, які впливають на глобальну безпеку та демократичні процеси.

Значний вплив кіберзагрози мають на такі фундаментальні права, як право на приватність, свобода слова та доступ до правосуддя. Незаконний збір, збереження та використання персональних даних, а також несанкціонований моніторинг комунікацій можуть порушувати право на приватне життя, гарантоване міжнародним правом. Також важливим аспектом є загроза свободі вираження поглядів, що виникає внаслідок як державної цензури, так і маніпуляцій у соціальних мережах, спрямованих на дезінформацію або розпалювання ворожнечі. У сфері доступу до правосуддя постає проблема ефективності розслідувань кіберзлочинів, зокрема з огляду на складність ідентифікації правопорушників та відсутність єдиних міжнародних стандартів у цій сфері.

Міжнародне право відіграє важливу роль у регулюванні кібербезпеки та захисту прав людини. Основні принципи, закріплені в міжнародних документах, таких як Міжнародний пакт про громадянські і політичні права, Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) та резолюції ООН, визначають правові рамки для забезпечення захисту прав і свобод людини в цифровому середовищі. У контексті міжнародного співробітництва важливими є ініціативи ООН, Європейського Союзу, Інтерполу та інших міжнародних організацій, спрямовані на створення ефективних механізмів протидії кіберзагрозам.

Важливою складовою забезпечення прав людини в умовах кіберзагроз є розробка глобальних стандартів кібербезпеки, що поєднують правозахисний підхід із вимогами національної безпеки. В умовах глобалізації та цифрової інтеграції міжнародна спільнота має адаптувати правові механізми до новітніх викликів, зокрема до питань кіберсуверенітету, штучного інтелекту, цифрової ідентифікації та криптовалют. Вирішення цих питань вимагатиме більшої координації між державами, а також розробки ефективних міжнародно-правових механізмів, які зможуть гарантувати захист основних прав і свобод людини у швидкозмінному кіберпросторі.

Ключові слова: кіберзагрози, права людини, міжнародне право, кібербезпека , кіберзлочинність, міжнародне співробітництво.

Постановка проблеми

Проблема міжнародного правового регулювання кібербезпеки та захисту прав людини полягає у необхідності створення ефективних механізмів, які б забезпечували баланс між безпекою та дотриманням фундаментальних прав у цифровому просторі. Зростання кіберзагроз загрожує приватності, свободі вираження думок та іншим правам людини, тоді як відсутність єдиного міжнародного підходу ускладнює правове реагування на ці виклики. Необхідність гармонізації національного та міжнародного законодавства щодо кіберзлочинності, захисту даних та регулювання цифрових технологій є ключовою умовою забезпечення ефективного правового захисту в умовах сучасного глобалізованого світу.

Аналіз останніх досліджень і публікацій

Аналіз останніх досліджень і публікацій на тему міжнародного правового регулювання кібербезпеки та захисту прав людини свідчить про зростаючий інтерес до правових механізмів реагування на кіберзагрози та забезпечення балансу між безпекою і правами людини в цифровому просторі. У працях таких вчених, як А. Пазюка, В. Шамрая, Р. Шаповала, Ч. Кеннеді, Дж. Куліша та інших, особливу увагу приділено питанням міжнародного співробітництва у сфері кібербезпеки, гармонізації національного законодавства із міжнародними стандартами та правовим аспектам захисту персональних даних і свободи вираження поглядів в умовах цифрової трансформації.

Мета і завдання дослідження

Мета дослідження полягає в аналізі сучасних кіберзагроз і їхнього впливу на права людини, а також в оцінці міжнародно-правових механізмів захисту прав людини в умовах цифрових загроз. Завданням є дослідити характер кіберзагроз, їх наслідки для прав індивідів та демократичних процесів, вивчити роль міжнародного права в захисті прав людини в кіберпросторі, а також проаналізувати ефективність міжнародного співробітництва в боротьбі з кіберзлочинністю і збереженням прав людини в умовах новітніх технологій.

Виклад основного матеріалу

Кіберзагрози є одними з найбільш серйозних викликів для сучасного суспільства, оскільки їхні наслідки можуть торкатися різних аспектів життя — від безпеки держави до прав індивідів. З розвитком цифрових технологій та інтеграцією Інтернету в усі сфери людської діяльності, питання захисту інформаційних систем, а також забезпечення прав і свобод громадян в умовах кіберзагроз набувають особливої актуальності. Сучасні кіберзагрози можуть охоплювати широкий спектр небезпек, від атак на критичну інфраструктуру та фінансові системи до порушення приватності через незаконний збір даних або маніпуляції з інформацією. Зокрема, порушення таких фундаментальних прав людини, як право на приватність, свобода вираження поглядів і доступ до правосуддя, може мати руйнівні наслідки для демократичних процесів та індивідуальних свобод.

В умовах глобалізації та швидкого розвитку інформаційних технологій, кіберзагрози стають не лише питанням національної безпеки, але й важливою складовою міжнародно-правової практики захисту прав людини. Оскільки кіберпростір не має чітких географічних меж, загрози можуть надходити від будь-якої країни, а наслідки торкаються глобальної спільноти. Міжнародне співробітництво і гармонізація правових підходів до забезпечення кібербезпеки є необхідними для мінімізації ризиків і захисту прав людини в умовах технологічних змін. З цієї причини питання міжнародно-правового регулювання кібербезпеки, зокрема в аспекті захисту прав людини, набуває все більшої важливості на світовій арені [1].

Кіберзагрози є серйозними і постійно зростаючими викликами для сучасного світу. Вони охоплюють широкий спектр негативних впливів на інтернет-простір і інформаційні системи, від кібератак на інфраструктуру держав до порушень прав людини через зловживання цифровими платформами. Окрім традиційних загроз, таких як зломи систем або фінансові махінації,

кіберзагрози можуть включати нові форми порушення прав, такі як витоки особистих даних, незаконний моніторинг інтернет-комунікацій або використання соціальних мереж для пропаганди насильства та тероризму. Завдяки глобальній мережі інтернет ці загрози можуть охоплювати мільйони людей по всьому світу, не маючи чітких меж.

Одним з найбільш болючих наслідків кіберзагроз є порушення права на приватність. Кібератаки, які включають незаконний збір, використання або продаж особистих даних, можуть призвести до серйозних порушень індивідуальних прав, зокрема, права на недоторканність особистого життя. Інші форми порушень, такі як масові витоки інформації або маніпуляції з особистими даними для політичних або економічних цілей, ставлять під загрозу основні принципи прав людини, зокрема захист від свавільного втручання в приватне життя.

Інший аспект кіберзагроз, який суттєво впливає на права людини, — це порушення свободи слова. Зловживання інтернет-платформами для поширення дезінформації, ненависті або насильства ставить під загрозу право на свободу вираження поглядів. Водночас держави, що прагнуть контролювати інформацію в інтернеті, можуть вдаватися до цензури, що обмежує доступ до інформації та порушує основні свободи, закріплені у міжнародних документах, таких як Міжнародний пакт про громадянські і політичні права. Питання цензури в кіберпросторі стає особливо актуальним в контексті політичних та соціальних кризи, де держави використовують технології для обмеження свободи вираження думок або придушення інакомислення.

Не менш важливим є питання доступу до правосуддя та захисту від насильства в цифровому середовищі. Кіберзагрози можуть спричинити труднощі в забезпеченні правосуддя для жертв кіберзлочинів або кібербулінгу. Законодавчі та правові механізми, що регулюють боротьбу з кіберзлочинністю, все ще знаходяться на стадії розвитку і часто не враховують новітні технології, такі як криптовалюти чи штучний інтелект, що ускладнює забезпечення справедливості. Водночас жертви кіберзлочинів, часто не маючи змоги ефективно захистити свої права, стикаються з численними юридичними бар'єрами, відсутністю доказової бази чи недостатньою правовою допомогою на міжнародному рівні.

Міжнародно-правовий підхід до цих питань намагається збалансувати забезпечення національної безпеки та захист прав громадян у кіберпросторі. Водночас важливою є роль міжнародного співробітництва для боротьби з кіберзагрозами. Оскільки кіберзлочини та кібернапади можуть мати міжнародний характер, координація дій на рівні держав та міжнародних організацій є необхідною для ефективної протидії цим загрозам. Проблеми кіберзагроз потребують комплексного підходу, що поєднує міжнародні стандарти, національні закони і механізми міжнародного співробітництва. Таким чином, для досягнення ефективного захисту прав людини в умовах кіберзагроз важливо розробляти глобальні правові стандарти, які враховуватимуть інтереси та потреби різних країн і спільнот [1].

У міжнародному праві існують кілька ключових документів, які визначають рамки захисту прав людини в умовах кіберзагроз. Одним з основних є Міжнародний пакт про громадянські і політичні права (МКГПП), який є фундаментальним інструментом для забезпечення основних прав і свобод людини. Зокрема, ст. 17 МКГПП гарантує право на захист від свавільних або незаконних втручань у приватне життя, сім'ю, житло або кореспонденцію, що безпосередньо стосується захисту приватності в цифровому середовищі. Стаття 19 цього ж Пакту закріплює право на свободу вираження думок і доступ до інформації, що є важливим у контексті кіберпростору, де порушення цього права може мати далекосяжні наслідки, зокрема у вигляді цензури або маніпуляцій з інформацією [2].

У 2013 році Генеральна Асамблея ООН прийняла Резолюцію 68/167, яка підкреслює важливість захисту прав людини в цифровому середовищі. Це був важливий крок у визнанні глобальних кіберзагроз як частини міжнародної правової практики щодо забезпечення прав людини. Резолюція наголошує на необхідності забезпечен-

ня доступу до правосуддя для осіб, чиї права порушуються через кіберзлочини, а також на необхідності протидії кібернападам та захисту прав на приватність в умовах швидко зростаючого використання цифрових технологій [3].

Міжнародне співтовариство визнає, що порушення прав людини в кіберпросторі може мати глобальні наслідки, оскільки інтернет не має географічних кордонів. Це ставить перед державами та міжнародними організаціями завдання розробити ефективні механізми захисту прав людини в умовах кіберзагроз, включаючи протидію кібертероризму, захист від незаконного збору та використання особистих даних, а також запобігання цензурі або обмеженням свободи вираження поглядів в інтернеті [4].

Резолюція ООН також наголошує на необхідності міжнародного співробітництва для боротьби з кіберзагрозами, що включає обмін інформацією між державами, координацію дій правоохоронних органів, а також розвиток стандартів кібербезпеки на глобальному рівні. Це співробітництво важливе не лише для забезпечення безпеки, а й для гарантування захисту прав людини в інтернет-просторі, що потребує узгодження національних законів з міжнародними стандартами.

Таким чином, міжнародне право, зокрема через такі документи, як МКГПП та резолюції ООН, відіграє ключову роль у формуванні правової основи для захисту прав людини в кіберпросторі. Однак, існує необхідність подальшої гармонізації національних законодавств із міжнародними стандартами, а також удосконалення механізмів захисту прав громадян у цифровому середовищі, що вимагає постійної адаптації до швидко змінюваного технологічного ландшафту [5].

Міжнародне співробітництво є критично важливим елементом для забезпечення ефективного захисту прав людини в умовах кіберзагроз. Кіберзлочинність не знає кордонів, і з цієї причини жодна країна не може боротися з цими загрозами самостійно. Тому міжнародні організації, такі як ООН, Європейський Союз (ЄС) та Інтерпол, відіграють важливу роль у створенні спільних стандартів і механізмів, спрямованих на захист прав людини в кіберпросторі.

Одним з основних напрямів співпраці між державами і міжнародними організаціями є розробка загальних правових рамок для боротьби з кіберзлочинністю, які охоплюють як кримінальні, так і правозахисні аспекти. У цьому контексті важливим міжнародним інструментом є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), яка була прийнята в 2001 році і є першою міжнародною угодою, що надає правову базу для боротьби з кіберзлочинністю. Будапештська конвенція стала основою для співпраці багатьох держав у боротьбі з кіберзлочинами, зокрема з комп'ютерними злочинами, кібертероризмом та іншими видами цифрових правопорушень. Вона також встановлює механізми міжнародної співпраці для збору доказів, екстрадиції злочинців та взаємного надання допомоги в розслідуваннях.

Ця конвенція підкреслює важливість обміну інформацією та координації зусиль між державами для ефективної боротьби з кіберзагрозами, не порушуючи при цьому основоположних прав людини. Наприклад, у межах Будапештської конвенції було досягнуто компромісу між необхідністю боротьби з кіберзлочинами та забезпеченням права на приватність, що є важливим аспектом захисту прав людини. Крім того, конвенція надає країнам можливість адаптувати національні законодавства до нових цифрових реалій та технологічних викликів [6].

Іншим важливим механізмом міжнародного співробітництва є ініціативи ООН, що включають розробку міжнародних стандартів щодо кібербезпеки та захисту прав людини в кіберпросторі. У 2015 році ООН прийняла резолюцію, яка підкреслює необхідність забезпечення прав людини в умовах цифрової революції та пропонує країнам розробляти національні стратегії для боротьби з кіберзагрозами, при цьому не порушуючи прав на свободу вираження думок та доступ до інформації. ООН також ініціювала створення Глобальної групи експертів з кібербезпеки, яка надає країнам рекомендації щодо створення ефективних політик для захисту прав людини в інтернеті.

Крім того, міжнародні організації, такі як Європейський Союз (ЄС), активно працюють над розробкою спільних правових актів, що регулюють кібербезпеку і захист прав людини в цифровому середовищі. ЄС активно впроваджує стратегії кібербезпеки, які включають заходи щодо захисту приватних даних, боротьби з кіберзлочинністю та просування цифрових прав у межах своїх країн-членів. Одним з таких інструментів є Регламент ЄС про захист даних (GDPR), який встановлює високі стандарти захисту особистої інформації в цифровому середовищі та має значний вплив на міжнародну практику захисту приватності [7].

Міжнародне співробітництво в боротьбі з кіберзагрозами також включає Інтерпол, який сприяє координації дій правоохоронних органів країн світу в боротьбі з кіберзлочинами. Інтерпол надає технічну і правову допомогу в розслідуваннях кіберзлочинів, а також організує міжнародні тренінги для поліцейських і фахівців у галузі кібербезпеки [8].

Таким чином, міжнародне співробітництво в захисті прав людини від кіберзагроз є важливою складовою глобальної стратегії боротьби з кіберзлочинністю. Спільні правові рамки та ефективна координація між державами і міжнародними організаціями дозволяють не лише знизити ризики кіберзагроз, але й забезпечити захист основних прав і свобод людини в умовах цифрової ери.

Перспективи розвитку міжнародного правового регулювання прав людини в умовах кіберзагроз зумовлені необхідністю постійного вдосконалення наявних механізмів і створення нових міжнародних стандартів, які зможуть адекватно реагувати на виклики сучасного цифрового середовища. Оскільки кіберзагрози продовжують швидко еволюціонувати, стає очевидним, що міжнародне право повинно розвиватися у відповідь на ці зміни, пропонуючи ефективні інструменти для захисту прав людини в умовах нових технологій.

Одним з важливих напрямків є розробка більш конкретних та дієвих стандартів для захисту прав людини в цифровому середовищі, зокрема щодо захисту персональних даних, приватності та свободи вираження думок в Інтернеті. Потреба в таких стандартах зумовлена швидким розвитком інформаційних технологій та загрозами, які вони створюють для індивідуальних прав. Тому створення глобальних принципів і юридичних норм для регулювання онлайн-простору стає необхідністю для забезпечення балансу між безпекою та правами людини.

Посилення співпраці між державами, міжнародними організаціями та приватним сектором є ще одним ключовим напрямком розвитку міжнародного правового регулювання кіберзагроз. Оскільки кіберзагрози є глобальними і не зупиняються на межах державних кордонів, міжнародна співпраця в цій сфері має бути системною і всеохоплюючою. Держави повинні працювати разом, обмінюючись інформацією та розробляючи спільні стратегії протидії кіберзлочинам. Приватний сектор, у свою чергу, відіграє важливу роль у забезпеченні безпеки в інтернет-просторі, особливо в аспектах технологічного розвитку та реалізації інноваційних рішень для захисту даних та інформації.

Одним із важливих аспектів майбутнього розвитку міжнародного правового регулювання є створення ефективних механізмів правосуддя для вирішення спорів щодо порушення прав людини в кіберпросторі. Оскільки інтернет дозволяє здійснювати порушення прав на глобальному рівні, забезпечення справедливості в цьому контексті потребує створення нових міжнародних інституцій або адаптації існуючих органів до специфіки кіберзагроз. Прозорі механізми для вирішення таких спорів допоможуть не тільки відновлювати порушені права, а й виступати як стримуючий фактор для потенційних порушників.

Важливо також зазначити, що майбутнє міжнародного правового регулювання кіберзагроз повинно враховувати новітні технології, зокрема штучний інтелект, блокчейн та інші. Ці технології ставлять нові виклики перед правовою системою, оскільки їх застосування може створювати не тільки нові можливості для покращення захисту прав людини, але й нові ризики, які потребують особливого правового регулювання. Тому важливо, щоб міжнародне право було

готове до швидкої адаптації до цих технологій, забезпечуючи їх використання в інтересах громадян та держав, але не в цілях порушення основоположних прав [9].

Висновки

Кіберзагрози є серйозною проблемою для сучасного суспільства, оскільки вони безпосередньо впливають на різні аспекти життя, зокрема на права людини. Вони загрожують приватності індивідів, можуть порушувати свободу слова та доступ до правосуддя, а також підривати демократичні процеси. Оскільки кіберпростір не має чітких географічних меж, кіберзагрози мають глобальний характер і потребують міжнародної координації та правового регулювання для забезпечення прав людини на міжнародному рівні.

Міжнародне співробітництво в боротьбі з кіберзагрозами є важливим для створення спільних правових стандартів і механізмів захисту прав людини в цифровому середовищі. Зокрема, міжнародні організації, такі як ООН та ЄС, працюють над розробкою стандартів кібербезпеки, що включають захист персональних даних, боротьбу з кіберзлочинністю та забезпечення свободи вираження думок. Тому розвиток міжнародного правового регулювання має бути спрямований на гармонізацію національних законів з міжнародними стандартами для ефективного протистояння кіберзагрозам і забезпечення прав людини в умовах технологічних змін.

Література

1. Pasupuleti M.K. Cyberlaw Essentials: Rights and Regulations in the Digital Age. Digital Law: Navigating Rights and Regulations in the Tech Era URL: https://www.researchgate.net/publication/379899814_Cyberlaw_Essentials_Rights_and_Regulations_in_the_Digital_Age

2. Міжнародний пакт про громадянські і політичні права URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

3. Resolution adopted by the General Assembly on 18 December 2013 № 68/167 URL: https://docs.un.org/en/A/RES/68/167

4. Absor A.M. Juridical Analysis of Human Rights Protection in the Era of Digital Transformation: Perspective of Laws and Regulations. Indonesia Media Law Review 2(2). 2023. URL: https://www.researchgate.net/publication/373843926_Juridical_Analysis_of_Human_Rights_Protection_in_the_Era_of_Digital_Transformation_Perspective_of_Laws_and_Regulations

5. Raynor J., Bah A., Brouillard T. Internet Regulation vs. Freedom of Speech: A Cyberlaw Case Study of Section 230 URL: https://www.researchgate.net/publication/352515923_Internet_Regulation_vs_Freedom_of_Speech_A_Cyberlaw_Case_Study_of_Section_230

6. Конвенція Ради Європи про кіберзлочинність URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

7. Регламент ЄС про захист даних (GDPR) URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

8. International cooperation on cybersecurity matters URL: https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

9. The Cyber World and Human Rights: Perspectives on International Accountability URL: https://www.stimson.org/2024/the-cyber-world-and-human-rights-perspectives-on-international-accountability/

Kotsiuruba Serhii,
graduate student of the Department of International and European Law
Faculty of Law and International Relations
State Non-Commercial Company «State University «Kyiv Aviation Institute»»
ORCID: 0009-0006-1741-4308

INTERNATIONAL LEGAL ASPECTS OF HUMAN RIGHTS PROTECTION IN THE CONTEXT OF CYBER THREATS

In today's world, cyber threats have become one of the key challenges to human rights, as they cover a wide range of risks, including the illegal collection and use of personal data, information manipulation, cyber attacks on critical infrastructure, and violations of freedom of expression. In the context of the digital transformation of society, there is a need to improve international legal mechanisms to

ensure human rights in cyberspace. This is due to both the rapid development of technology and the growing number of cyber incidents that affect global security and democratic processes.

Cyber threats have a significant impact on such fundamental rights as the right to privacy, freedom of speech and access to justice. The unlawful collection, storage and use of personal data, as well as unauthorized monitoring of communications, may violate the right to privacy guaranteed by international law. Another important aspect is the threat to freedom of expression arising from both state censorship and manipulation of social media aimed at disinformation or hate speech. In the area of access to justice, there is a problem with the effectiveness of cybercrime investigations, in particular given the difficulty of identifying offenders and the lack of uniform international standards in this area.

International law plays an important role in regulating cybersecurity and protecting human rights. The basic principles enshrined in international documents, such as the International Covenant on Civil and Political Rights, the Council of Europe Convention on Cybercrime (Budapest Convention), and UN resolutions, define the legal framework for ensuring the protection of human rights and freedoms in the digital environment. In the context of international cooperation, the initiatives of the UN, the European Union, Interpol and other international organizations aimed at creating effective mechanisms to counter cyber threats are important.

An important component of ensuring human rights in the context of cyber threats is the development of global cybersecurity standards that combine a human rights-based approach with national security requirements. In the context of globalization and digital integration, the international community must adapt legal mechanisms to the latest challenges, including cybersovereignty, artificial intelligence, digital identification, and cryptocurrencies. Addressing these issues will require greater coordination between states, as well as the development of effective international legal mechanisms that can guarantee the protection of fundamental human rights and freedoms in the rapidly changing cyberspace.

Key words: cyber threats, human rights, international law, cybersecurity, cybercrime, international cooperation.