DOI https://doi.org/10.30525/978-9934-26-432-0-36

# THE ROLE OF INTERNATIONAL ORGANIZATIONS IN ENSURING THE PROTECTION OF HUMAN RIGHTS IN CYBER SPACE

# РОЛЬ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ У ЗАБЕЗПЕЧЕННІ ЗАХИСТУ ПРАВ ЛЮДИНИ В КІБЕРПРОСТОРІ

**Paseshnyk O. R.**
*Postgraduate student at the Department of International, Civil and Commercial Law*
*State University of Trade and Economics*
*Kyiv, Ukraine*

**Пасешник О. Р.**
*аспірант кафедри міжнародного, цивільного та комерційного права*
*Державний торговельно-економічний університет*
*м. Київ, Україна*

На сучасному етапі міжнародні організації відіграють ключову роль у формуванні міжнародного правопорядку та забезпеченні захисту прав людини. Вони є невід'ємною частиною системи захисту прав людини і саме в рамках міжнародних організацій були прийняті основні документи прав та свобод людини: Загальна декларація прав людини 1948 року, Конвенція про захист прав людини та основоположних свобод 1950 року, Міжнародний пакт про громадянські і політичні права 1966 року, Міжнародний пакт про економічні, соціальні та культурні права 1966 року, Конвенція про ліквідацію всіх форм расової дискримінації 1965 року, та низка інших документів прийнятих на різних рівнях.

Однією з основних організацій є Організація Об'єднаних Націй, яка відіграє ключову роль у контексті забезпечення миру і безпеки та захисті прав людини. Під егідою ООН діє Управління Верховного комісара з прав людини, Рада з прав людини, Договірні органи з прав людини. Крім того, в рамках ООН діють незалежні експерти, які регулярно досліджують ситуації пов'язанні з захистом прав людини в різних регіонах. Зокрема, такі організації не залишаються осторонь у питаннях захисту прав і свобод людини у кіберпросторі.

З розвитком технологій стає очевидним, що захист прав людини повинен охоплювати не лише їх реальне життя, а також їх активність у кіберпросторі. Саме тому ООН активно поглиблює свій вплив

на захист людей у рамках кібербезпеки. В ООН існує Управління по боротьбі з тероризмом, в рамках якого з квітня 2020 року діє програма: «Кібербезпека та нові технології», яка підтримує стратегічне зобов'язання ООН створити світ без тероризму, вона підтримується шляхом активної співпраці з такими партнерами, як Міжнародний союз електрозв'язку, Міжнародна організація кримінальної поліції, Організація з безпеки та співробітництва у Європі та ще ряд інших організацій і департаментів. Разом вони забезпечують розвиток знань та підвищення обізнаності про виклики та можливості, пов'язанні з новими технологіями у протидії тероризму, підвищення навичок необхідних для розробки ефективної національної антитерористичної політики, покращення навичок і можливостей необхідних для захисту критичної інфраструктури від кібератак, а також допомагають у розширені норм кримінального правосуддя [1].

Вагомою організацією є ОБСЄ – Організація з безпеки і співробітництва у Європі. Одним із головних векторів діяльності ОБСЄ є захист від кіберзагроз. Його структурні органи регулярно роблять звіти, проводять тренінги, підвищують обізнаність у цих питання, а також проводять конференції на яких активно обговорюють питання пов'язанні з такими загрозами. Більше того, ОБСЄ не стоїть осторонь питань захисту критичної інфраструктури від кібератак. У 2017 році була проведена конференція «Кібербезпека для критичної інфраструктури: посилення розбудови довіри в ОБСЄ» та навчання пов'язанні з таким захистом, прикладом таких навчань є Боснія та Герцеговина, в якій у 2018 році ОБСЄ провела національні масові навчання щодо захисту критично важливої енергетичної інфраструктури.

У контексті захисту кіберпростору ОБСЄ виконує стримуючу роль між державами. Більшість держав активно розвивають свої інформаційно-комунікаційні технології, що призводить до конфліктів між країнами. В свою чергу, країни-учасниці ОБСЄ працюють над заходами зміцнення довіри, щоб зменшити ризики конфліктів пов'язанні з використанням таких технологій. Вони пропонують конкретні інструменти та механізми, а саме: механізм об'єднання держав для консультацій щодо потенційних інцидентів у сфері кібербезпеки, надають платформу для обміну думками, національною політикою, що допоможе державам краще розуміти наміри один одної в кіберпросторі, а також, надає конкретні завдання, як приклад, для захисту критичної інфраструктури яка працює на основі інформаційно-комунікаційних технологій. Поміж іншого, вони також зосереджені на боротьбі з загрозами з боку недержавних суб'єктів, які реалізуються

шляхом сприяння своєчасним реакціям з боку національних органів влади на такі загрози [2].

Інтерпол, як міжнародна організація кримінальної поліції є ключовою установою у попередженні та боротьбі з кіберзлочинністю, вона включає в себе 196 країн, надає підтримку в проведенні розслідувань і допомогу в розшуку втікачів по всьому світу. Організація активно проводить кооперації з різними регіонами світу задля захисту від кібератак та боротьбі з кіберзлочинністю, в рамках такої кооперації був створений проект AFJOC – Африканська спільна операція проти кіберзлочинності. Основна ідея полягає у тому, що в Африці йде активна цифровізація і виникла потреба розвивати протоколи кіберзахисту. Іншим прикладом є Відділ операцій з кіберзлочинності ACEAN (Асоціація держав Південно-Східної Азії), який спрямований на координацію спільних зусиль країн регіону проти кіберзлочинності. Інтерпол має п'ять регіональних робочих груп з кіберзлочинністю в Америці, Африці, Азії, Європі та на Близькому Сході. Ціллю таких груп є моніторинг ситуацій пов'язаних з кіберзлочинністю, обмін досвідом та консультації щодо розробки методів захисту від кібератак.

Інтерпол приділяє велику увагу розширенню партнерства у сфері кіберзахисту. Організація заохочує до співпраці інші організації і приватний сектор, вважаючи, що така співпраця може принести більше користі ніж співпраця з країнами через їх закритість, а також через те, що приватні компанії активно розвивають свої власні технології боротьби та активно стикаються з різними видами кібератак на свої системи.

У рамках забезпечення безпеки Інтерпол розробив 7 основних глобальних цілей цієї організації, однією з яких є зменшити глобальний вплив та шкоду від кіберзлочинності. Для досягнення цих цілей був розроблений стратегічний план дій з 2022 року по 2025 рік, відповідно якому вони поставили для себе 4 основні цілі у боротьбі з кіберзлочинністю:

1. Забезпечення проактивної та гнучкої позиції у запобіганні та протидії кіберзлочинності шляхом розвитку глибокого розуміння ландшафту загроз кіберзлочинності за допомогою обміну інформацією та аналізу розвідувальних даних.

2. Ефективно запобігати, виявляти, розслідувати та припиняти кіберзлочинність, яка завдає значної шкоди на національному, регіональному та глобальному рівнях, очолюючи, координуючи та підтримуючи країни-члени у транснаціональній оперативній діяльності.

3. Підтримувати розвиток стратегій і можливостей країн-членів у боротьбі з кіберзлочинністю шляхом розвитку відкритих, інклюзивних і різноманітних партнерств, а також зміцнення довіри до глобальної екосистеми кібербезпеки.

4. Сприяти підвищенню ролі та можливостей Інтерполу у формуванні глобальної безпеки шляхом взаємодії з міжнародними форумами у сфері кіберзлочинності [3].

Міжнародні організації відіграють надзвичайно важливу роль у забезпеченні прав і свобод людини в кіберпросторі. Кожна з цих організацій має досить широкий обсяг роботи спрямований на захист людей у цифровому середовищі. В глобальному плані, всі вони забезпечують захист прав і свобод людини, але кожна з них має своє власне бачення як краще запровадити такий захист – від створення нормативних документів, моніторингу та аналізу, до допомоги конкретним країнам у запобіганні злочинів. Часто такі організації кооперуються задля забезпечення правопорядку у всьому світі та сприянню виконанню поставлених цілей і захисту як звичайних людей так і цілих країн. Спільна робота дозволяє реалізувати стратегії та програми з кібербезпеки на міжнародному рівні, забезпечуючи стабільність, безпеку та захищеність в цифровому просторі. Інтернаціональне співробітництво в цій сфері є критично важливим аспектом у боротьбі з кіберзагрозами та забезпеченні захисту прав людини в Інтернеті.

**Література:**

1. Cybersecurity and New Technologies // United Nations. URL: https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity (дата звернення 05.03.2024).

2. Cyber/ICT Security // Organization for Security and Co-operation in Europe. URL: https://www.osce.org/cyber-ict-security (дата звернення 06.03.2024).

3. Strategic Framework 2022–2025 // Interpol. URL: https://www.interpol.int/Who-we-are/Strategy/Strategic-Framework-2022-2025 (дата звернення 10.03.2024).