УДК 327
DOI: https://doi.org/10.17721/1728-2292.2024/2-59/41-44

Ярослав ПЕТІК, магістр, старш. наук. співроб.
ORCID ID: 0000-0002-6127-5943
e-mail: iaroslav.petik@gmail.com
Музей видатних діячів української культури Лесі Українки,
Миколи Лисенка, Панаса Саксаганського, Михайла Старицького, Київ, Україна

# ОГЛЯД ЗАСІДАНЬ ВІДКРИТОЇ РОБОЧОЇ ГРУПИ ООН ЩОДО БЕЗПЕКИ В КІБЕРПРОСТОРІ НА ФОНІ ВІЙНИ В УКРАЇНІ В 2023 РОЦІ

**Вступ.** *Четверте та П'те засідання Відкритої Робочої групи ООН зачепило проблеми безпекової політики в кіберпросторі. Процес вироблення юридичних механізмів був ускладнений політизованою дискусією, в якій брала участь Росія маючи на увазі свої геополітичні інтереси на фоні війни в Україні, яка продовжується.*

**Методи.** *Застосовані такі методи, як аналіз матеріалів, публікацій і аналітичних звітів, міждисциплінарний підхід (аналіз міжнародного права, дипломатичних документів, технічних аспектів кіберзахисту й геополітичного контексту), порівняльний аналіз, контент-аналіз текстів, використання вторинних джерел (наукових статей і аналітичних звітів).*

**Результати.** *Було розглянуто результати згаданих засідань, підкреслено геополітичний контекст обговорень та дані прогнози щодо розвитку безпекової політики в кіберпросторі.*

**Висновки.** *Визначено основні проблемні точки в дискусіях між різними делегаціями під час засідань Робочої групи. Було висвітлено як геополітичні інтереси Росії стосовно безпекової політики в кіберпросторі, так і деякі інтереси інших країн. Обговорення питання кібербезпеки було пов'язано із проблемами політичної суверенності та принципу не втручання, що є важливими класичними проблемами міжнародних відносин. Як висновок, постулювалася необхідність подальшого розвитку юридичних норм і механізмів, які б регулювали безпеку в кіберпросторі.*

**Ключові слова:** *кібербезпека, Робоча Група ООН, війна в Україні, геополітика, міжнародні відносини, дипломатія, кіберпростір, Росія.*

## Вступ

У статті розглядатимуться результати Четвертого та П'ятого засідань Відкритої Робочої групи ООН (UN Open-Ended Working Group (OEWG)), зокрема, результати дискусій щодо безпеки в кіберпросторі. Сесії Групи відбулися 2023 р. і матимуть суттєвий вплив на міжнародну політику у відповідній сфері. Засідання були сильно політизовані через військовий конфлікт в Україні, який продовжується і дотепер. Це стосується не тільки "класичних" проблем міжнародних відносин та гуманітарного права, а також комп'ютерних технологій. Вторгнення Росії в Україну в 2022 р., окрім потужного військового протистояння, запустило справжнє протистояння хакерів і хактивістів з обох сторін у кіберпросторі.

Зокрема, на засіданнях виступали представники Росії та Білорусі, а також союзних країн, які вимагали уточнень ситуації використання принципу міжнародного гуманітарного права (МГП) до безпеки в кіберпросторі. Логічним здається, що принципи МГП мають застосовуватись у цій сфері хіба що з певними технічними уточненнями, але через виникле протистояння обговорення були сильно ускладнені.

Інтрига тут у тому, що Росія та її союзники одночасно хочуть зберегти право втручання у питання внутрішньої безпеки стосовно цензури в соціальних мережах і розповсюдження інформації в цілому на своїй території, і при цьому уникати відповідальності за дії своїх хакерів у міжнародному кіберпросторі. Дискусія звелася до визначення поняття суверенності держави щодо кіберпростору.

## Методи

Дослідження побудоване на основі аналізу матеріалів, публікацій та аналітичних звітів. Для висвітлення тематики кібербезпеки використовувалися міждисциплінарні підходи, що поєднують аналіз міжнародного права, дипломатичних документів, технічних аспектів кіберзахисту й геополітичного контексту.

Застосовано методи порівняльного аналізу з метою визначення основних розбіжностей у позиціях держав-учасників та оцінення впливу геополітичної ситуації на процеси обговорення. Додатково використано контент-аналіз текстів, щоб виявити тенденції та пріоритети у підходах до регулювання кіберпростору. Для контекстуалізації результатів використовувалися такі вторинні джерела, як наукові статті й аналітичні звіти, що розглядають кібербезпеку у світлі міжнародних відносин і конфліктів. Це дозволило оцінити унікальність ситуації, пов'язаної з війною в Україні, у ширшому контексті міжнародного правового регулювання.

***Мета.*** Метою статті є огляд і аналіз результатів конкретних засідань робочої групи ООН, які мають серйозний вплив на політику міжнародного регулювання безпеки в кіберпросторі. Ця політика важлива на фоні таких сучасних викликів, як кібертероризм, діджиталізація економіки та, зокрема, російського вторгнення в Україну.

***Огляд літератури.*** Засідання відкритої Робочої групи ООН аналізувалося в західній літературі, а саме спеціалістами НАТО з міжнародної політики та кібербезпеки (Kajander, 2023, p. 5). Загалом, проблема кібербезпеки та втручань у роботу інформаційної інфраструктури на міждержавному рівні аналізується в багатьох літературних джерелах (Korzak, 2021). Активності елітних хакерів, які традиційно асоціюються із ФСБ Росії або військовою розвідкою, також присвячено деякі публікації (Geers, 2015).

Зауважимо, що в існуючій літературі, на жаль, немає синтезованого розгляду як політико-правових, так і технічних аспектів регуляції кіберпростору. Саме цей пробіл намагається заповнити дана стаття.

## Результати

Не дивлячись на загальну політизованість дискусії та зіткнення геополітичних інтересів різних блоків держав щодо безпеки в кіберпросторі, засідання Робочої групи ООН винесли важливі рішення стосовно правового регулювання такого простору. Законодавство навіть розвинених країн ще далеке від ефективного контролю та захисту населення від загроз, які походять з кіберпростору. Крім того, як показує практика, таке регулювання має розроблятися саме на міжнародному рівні. Таким чином, ці засідання були важливими кроками в розвитку юридичної інтерпретації проблем кібербезпеки.



ISSN 1728-2292 (Print)

Проте саме ця необхідність міжнародної співпраці додає складнощів процесу. Кіберпростір надзвичайно важливий у політичному плані, і в майбутньому геополітичний вплив його правового регулювання тільки зростатиме. У даній конкретній ситуації Росія, Білорусь та інші країни, яким вигідно, щоб правові норми щодо кіберпростору залишалися розмитими, а контроль з питань інформаційної політики залишався виключно в національної держави, суттєво ускладнили перебіг засідань Робочої групи. Логіка соціального й технічного поступу однозначно вказує на необхідність створення прозорих засад юридичного регулювання цієї сфери саме на міжнародному рівні з плюралістичним поглядом на розповсюдження інформації та комп'ютерних технологій. Однак для класичної національної держави з авторитарним типом управління участь у такій системі майже неможлива.

Чим менше в країні демократії, чим сильніший нахил у бік консервативного суспільного устрою та традиційних цінностей, тим більше необхідно контролювати комунікацію й поширення інформації в соціальних мережах. Інакше авторитарний режим просто не виживе, адже без цензури на цих платформах поширюватимуться політичні ідеї та маніфести, організовуватметься опозиція.

Особливо загострилася ця проблема на фоні війни в Україні, яка продовжується. Росія намагається ускладнити процес переговорів у міжнародних організаціях не тільки з безпосередніх причин, які стосуються предмета переговорів, а також у ході загальної політики створення альтернативного полюса впливу в міжнародній дипломатії. В умовах міжнародної ізоляції, яка наявна після вторгнення 2022 р., така активність стає ще більш важливою для цієї країни.

Було згадано про протистояння ІТ-фахівців по обидва боки лінії фронту. Хакери крадуть інформацію, організовують диверсії (у т. ч. проти важливої військової та цивільної інфраструктури), проводять Ddoss-атаки, які суттєво ускладнюють публічну комунікацію ворога. Діють не тільки просунуті технічні спеціалісти. Громадяни обох країн прилучаються до масованих атак на ворожі ресурси з патріотичних міркувань у масштабах, які важко було б уявити у інших обставинах. Їх називають хактивістами. Це призвело до ситуації, коли війну України та Росії у фазі після вторгнення 2022 р. називають також початком першої глобальної кібервійни.

Дії та заяви Російської Федерації під час участі в обговоренні були насамперед направлені на те, щоб саботувати процедуру застосування міжнародного гуманітарного права до проблем кібербезпеки. Це виражене негативне явище, але воно створює дуже цікавий політико-дипломатичний прецедент, який заслуговує на глибоке дослідження. Воно особливо важливе в горизонті всезростаючого політичного значення ІТ-технологій.

Політика, зокрема світова, поступово сильніше переплітається з високими технологіями, особливо з комп'ютерами та комп'ютерними мережами. Це створює нові виклики й тенденції (приміром, у дипломатії), а також простір для переосмислення застосування міжнародного права.

**Дискусія і висновки**

Четверте засідання Відкритої Робочої групи було присвячено кільком різноманітним питанням міжнародної політики та відносин, із яких кібербезпека була лише одним пунктом. Проте через специфіку самого питання всі інші пункти порядку денного також впливали на це обговорення. Інші параграфи містили питання стосовно застосування міжнародного гуманітарного права та політичної суверенності національної держави, а також мирне обговорення гострих дискусійних тем. Зокрема, як уже згадувалося, розглядалося питання застосування міжнародного гуманітарного права в кіберпросторі. Під час обговорення виступили члени делегації Росії. Вони висунули твердження, що МГП не може бути автоматично застосовано до цієї сфери і необхідно розробити окремий документ, який би її регулював. Використання міжнародного гуманітарного права до кібербезпеки, наприклад, обмежило би дії військових хакерів щодо атак на об'єкти цивільної інформаційної інфраструктури.

В одному з попередніх розділів уже наводилися можливі причини, які спонукали російську делегацію висловити подібну позицію. Російські розвідувальні служби давно приділяють серйозну увагу розвитку своєї ІТ-інфраструктури, відбору людей у спеціальні відділи, які займаються внутрішньою кібербезпекою та атакують мережі противників, до яких належить і наша країна. При застосуванні МГП ця активність російської розвідки була би серйозно ускладнена, оскільки подібні атаки розцінювалися б як порушення міжнародного права.

Одним з найвідоміших випадків застосування Російською Федерацією своїх можливостей у кіберпросторі є втручання у вибори президента Сполучених Штатів Америки 2016 р. Були зафіксовані масовані інформаційні кампанії в соціальних мережах, робота ботів, які створювали потрібну суспільну думку, а також інформаційні "вкиди" стосовно внутрішніх політичних проблем США, які поляризували суспільство. Уважається, що ця інформаційна активність сильно вплинула на обрання наступним президентом США саме Дональда Трампа. Розслідування щодо цієї кампанії сильно вплинуло на світову інформаційну політику та політику безпеки в кіберпросторі.

Безсумнівно, російські спеціальні служби проводять операції з більш глибоким застосуванням комп'ютерних технологій, однак більшість із них залишаються таємними. Серед небагатьох відомих наслідків таких заходів варто згадати масштабну атаку на оператора мобільного зв'язку "Київстар" у 2023 р.

Щодо контролю інформації на власній території, то тут все більш прозоро. Соціальні мережі використовуються для поширення пропагандистських меседжів різними політичним силами, організації політичних акцій, політичних дискусій та обговорень. Звичайно, авторитарний режим прагне забезпечувати цензуру й політичний контроль у такому інформаційному середовищі.

У позиції Росії стосовно створення нового документа, який би регулював застосування права у сфері кібербезпеки відслідковується очевидне прагнення затягнути процес кодифікації права й максимально розмити правові норми, які тягнуть за собою відповідальність за порушення міжнародного гуманітарного права. Як відомо, МГП пропагує безпеку цивільної інфраструктури та вільний доступ до необхідних послуг цивільного некомбатантського населення. В умовах кіберпростору це б означало, що не можна вводити надто посилену інформаційну цензуру, а також атакувати інформаційні ресурси, які пов'язані з комунікацією та наданням необхідних інформаційних послуг цивільним.

Авторитарному режиму необхідно, щоб міжнародне право у сфері кібербезпеки залишалось нерозвиненим. Тоді є простір для політичних маневрів й уникнення відповідальності за порушення МГП. Для цього дискусія затягується і висуваються твердження про порушення

внутрішньої безпекової політики країни через введення таких норм. Це також видно з обговорення принципу суверенності національної держави.

Утім на певному етапі до заяв Росії щодо необхідності чіткішого формулювання правових норм доєдналися й інші держави. Якщо статус Білорусі як політичного союзника зрозумілий, то деякі інші держави, які виступили на підтримку розробки нового правового кодексу стосовно кібербезпеки мають власні інтереси. Наприклад Іран, як ультраконсервативне суспільство, дуже занепокоєний політикою розповсюдження інформації в соціальних мережах, оскільки окрім політичної цензури має забезпечувати домінування авторитету релігійного інститута в публічному дискурсі.

В основному претензії до МГП у кіберпросторі висловлювалися учасниками на тлі проблеми суверенності. Яким чином визначати суверенний кіберпростір національної держави? "Таллінський Посібник" (Tallinn Manual) – спеціальний документ, що створений експертами, які співпрацювали з НАТО для визначення й міжнародного реагування на кіберзагрози та конфлікти – дає певні загальні юридичні категорії. Але тут є багато важливих тонкощів.

Зокрема, виділяються різні рівні ІТ-інфраструктури, такі як фізичне "залізо" (hardware), логічний компонент (програмне забезпечення та пристрої для мережевих обмінів даними), а також соціальний (користувачі комп'ютерів). Які елементи кожного з рівнів уважати визначальними щодо суверенного права національної держави втручатися в інформаційну інфраструктуру?

Допустимо ситуацію, коли розташування апаратних компонентів є визначальним стосовно урядового втручання. Місце розташування сервера чи клієнтського терміналу визначає юрисдикцію правоохоронних органів. Це одразу створює масу проблем щодо боротьби з кіберзлочинністю. Що робити, якщо злочинці спеціально розміщують сервер з компрометуючими матеріалами у країні, в якій ускладнено проведення правоохоронних процедур через місцеве законодавство? Як бути з міжнародними угрупованнями, які можуть використовувати різні сервери й термінали в різних країнах? Як стосовно хмарних обчислень? Або протоколів обміну даними, які не використовують клієнт-серверну модель, наприклад peer-to-peer?

Крім того, треба враховувати, що технічно просунені користувачі легко знайдуть можливість обходити правові норми, які так примітивно трактують суверенність: розміщуватимуть сервери у відповідних географічних зонах, використовуватимуть інші технології під час обміну даними. На жаль, в Україні до сьогодні законодавство погано пристосовано для того, щоб боротися навіть з базовим медіапіратством, не кажучи вже про кіберзлочинність чи ворожих хакерів. Світове та європейське законодавство є трохи більш розробленим, але теж має чимало проблемних моментів.

Єдиний логічний вихід із цієї ситуації – брати до уваги не тільки апаратне забезпечення комп'ютерних мереж, а й інші рівні, зазначені у "Талліннському Посібнику". Це призводить до гострої дискусії, адже тоді система класифікації кіберзлочинів і визначення юрисдикції правоохоронних органів стає більш складною, такою, що її майже неможливо розглядати в цілому, без детального аналізу кожного окремого випадку.

Не дивлячись на згадану політизованість дискусії, треба враховувати, що суверенність національної державності є важливою проблемою міжнародних відносин. Виконання цього аспекту має дотримуватися в сучасній системі міжнародної політики. Свої пропозиції щодо цього питання стосовно кібербезпеки заявляли й інші держави, які важко запідозрити в симпатіях до Російської Федерації. Наприклад, Швейцарія та Сполучене Королівство. Суверенність тісно повязана з принципом не втручання в міжнародну політику.

Особливо важкими ці проблеми стають у контексті співпраці країн-учасниць ООН задля досягнення міжнародної безпеки. Міжнародні організації, пов'язані з дотриманням правил та норм безпеки, сильно впливають на відносини між країнами. У межах цих відносин потрібно визначити юрисдикцію як національної держави, так і згаданих міжнародних організацій. Неминучими є конфлікти інтересів. Для запобігання цьому, чи., принаймні, пом'якшення їхнього впливу, необхідно розробити чіткі й логічні механізми вирішення таких конфліктів.

Як показує історія таких міжнародних безпекових організацій, як Інтерпол, відсутність політичного консенсусу в міжнародних політичних відносинах може чинити руйнівний вплив на розробку та впровадження таких механізмів і підтримки стабільності у світі. На сьогодні головним чинником відсутності політичної стабільності залишається широкомасштабна російська війна проти України.

Окрім класичних проблем міжнародної безпеки, пов'язаних з відкритим військовим протистоянням, у цього конфлікту є негативні наслідки для світової дипломатії. Навіть із результатів засідань, розглянутих у цій статті, очевидно, що делегація Росії має на меті такі геополітичні цілі, як підтримка багатополярності у світі на противагу домінуванню США в міжнародних відносинах. Фактично нагальні проблеми національної та світової безпеки приносяться в жертву заради політичних амбіцій Росії та союзних країн.

Україна теж має докладати зусиль для нейтралізації впливу свого супротивника не тільки в колі питань щодо вторгнення, а й стосовно російських геополітичних амбіцій. Це можна зробити, висловлюючи свою позицію щодо розробки документів, які регулюють сферу кіберпростору зокрема. Крім того, безпека в кіберпросторі є надзвичайно важливою складовою загальної безпеки в країні та регіоні, а отже, засідання Відкритої робочої Групи, що розглядаються в цій статті, є важливими для української дипломатичної спільноти.

Підсумовуючи, можна сказати таке. Комп'ютерні технології і надалі стрімко розвиватимуться. Це створює надзвичайно складні виклики для права, правоохоронної системи, міжнародних відносин. Необхідно постійно вдосконалювати кодекси й набувати досвіду безпосереднього регулювання кіберпростору. Крім того, потрібно брати до уваги геополітичну обстановку, проблеми відносин конкретних національних держав і кіберзлочинність, що пов'язана з політикою. Тільки у такий спосіб можна забезпечити соціальний поступ і безпеку для світової спільноти.

**Список використаних джерел**

Geers, K. (Ed.). (2015). *Cyber War in Perspective: Russian Aggression against Ukraine.* NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

Kajander, A. (2023). *A Tale of Two Draft Resolutions: A Report on the Polarising International Law Discussions at the 2023 OEWG Substantive Sessions.* NATO CCD COE Publications. https://ccdcoe.org/library/publications/a-tale-of-two-draft-resolutions-a-report-on-the-polarizing-international-law-discussions-at-the-2023-oewg-substantive-session/

Korzak, E. (2021). *Tallinn Paper: Russia's Cyber Policy Efforts in the United Nations.* NATO CCD COE Publications. https://ccdcoe.org/library/publications/russias-cyber-policy-efforts-in-the-united-nations

**References**

Geers, K. (Ed.). (2015). *Cyber War in Perspective: Russian Aggression against Ukraine*. NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf

Kajander, A. (2023). *A Tale of Two Draft Resolutions: A Report on the Polarising International Law Discussions at the 2023 OEWG Substantive Sessions.* NATO CCD COE Publications. https://ccdcoe.org/library/publications/a-tale-of-two-draft-resolutions-a-report-on-the-polarizing-international-law-/discussions-at-the-2023-oewg-substantive-session/

Korzak, E. (2021). *Tallinn Paper: Russia's Cyber Policy Efforts in the United Nations.* NATO CCD COE Publications. https://ccdcoe.org/library/publications/russias-cyber-policy-efforts-in-the-united-nations

**Отримано редакцією журналу / Received: 20.07.24**
**Прорецензовано / Revised: 23.08.24**
**Схвалено до друку / Accepted: 26.11.24**

**Iaroslav PETIK, Senior Research**
**ORCID ID: 0000-0002-6127-5943**
**e-mail: iaroslav.petik@gmail.com**
**Museum of Prominent Figures of Ukrainian Culture of**
**Lesya Ukrainka, Mykola Lysenko,**
**Panas Saksahansky, Mykhailo Starytsky, Kyiv, Ukraine**

## REVIEW OF THE MEETINGS OF THE UNITED NATIONS OPEN WORKING GROUP ON CYBERSECURITY WITH THE WAR IN UKRAINE AS A BACKGROUND IN 2023

**Background.** ***The fourth and fifth meetings of the United Nations Open Working Group addressed issues of cybersecurity policy. The process of developing legal mechanisms was complicated by politicized discussions, with Russia participating with its geopolitical interests in mind against the backdrop of the ongoing war in Ukraine.***

**Methods.** ***The study employed methods such as the analysis of materials, publications, and analytical reports, an interdisciplinary approach (analyzing international law, diplomatic documents, technical aspects of cyber defense, and the geopolitical context), comparative analysis, content analysis of texts, and the use of secondary sources (scientific articles and analytical reports).***

**Results.** ***The outcomes of the mentioned meetings were reviewed, emphasizing the geopolitical context of the discussions and providing forecasts regarding the development of cybersecurity policy.***

**Conclusions.** ***The main problematic points in the discussions among different delegations during the Working Group meetings were considered. Both Russia's geopolitical interests regarding cybersecurity policy and some interests of other countries were highlighted. The discussion of cybersecurity issues was linked to problems of political sovereignty and the principle of non-interference, which are important classical issues in international relations. As a conclusion, the necessity of further development of legal norms and mechanisms regulating cybersecurity was postulated.***

**Keywords:** ***cybersecurity, United Nations Working Group, war in Ukraine, geopolitics, international relations, diplomacy, cyberspace, Russia.***

Автор заявляє про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The author declares no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.