Беренюк В. М.,
здобувач вищої освіти,
Національна академія Служби безпеки України
(м. Київ, Україна)

Слісаренко Т. В.,
здобувач вищої освіти,
Національна академія Служби безпеки України
(м. Київ, Україна)

Яковенко Н. В.,
старший викладач кафедри романо-германських мов,
Національна академія Служби безпеки України
(м. Київ, Україна)

РОЛЬ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ ТА КІБЕРАТАКАМ

Сучасні гібридні загрози характеризуються поєднанням військових і невійськових засобів – інформаційних, економічних, політичних і кібероперацій, – які російська федерація активно застосовує проти України. Такі загрози виходять за межі національних кордонів і можуть мати глобальні наслідки, що зумовлює необхідність скоординованих дій з боку багатьох держав і міжнародних організацій. Міжнародне співробітництво у цій сфері створює можливості для ефективного обміну розвідувальною інформацією, координації санкційної політики, проведення спільних навчань, а також розроблення єдиних правових і технічних стандартів безпеки.

Гібридні загрози визначаються як «загрози, створені супротивниками, здатними одночасно застосовувати традиційні та нетрадиційні засоби впливу». Вони поєднують примусові та підривні методи, зокрема диверсії, інформаційно-психологічні операції, енергетичний шантаж і кібератаки. Відповідно до українського законодавства, кібератака – це навмисні дії в кіберпросторі, спрямовані на порушення конфіденційності, цілісності чи доступності інформаційних ресурсів або на отримання несанкціонованого доступу до них. Таким чином, кібероперації є невід'ємною складовою гібридної війни, оскільки створюють дестабілізаційні ефекти нижче порогу відкритої воєнної агресії [1].

Гібридні загрози та кібернетичні атаки набули глобального масштабу. У світовій практиці визнано, що існуючі міжнародні норми та механізми потребують оновлення. У межах діяльності Групи урядових екпертів (GGE) ООН тривають обговорення щодо застосування міжнародного права в кіберпросторі.

У 2021 р. Генеральна Асамблея ООН ухвалила резолюцію з питань кібербезпеки, яка акцентує увагу на співпраці у протидії кібершахрайству і кіберзлочинності. Важливу роль відіграє також Відкрита робоча група ООН з питань безпеки в кіберпросторі (OEWG), яка розробила рекомендації щодо прозорості та обміну даними. Крім того, міжнародні правоохоронні структури (Interpol, Europol) також посилюють співпрацю для розслідування транснаціональних кібератак та гібридних операцій. Загалом міжнародний контекст визначається потребою створення ефективних спільних рамок - від гармонізації законодавства до обміну технічними індикаторами атак [2].

ООН виступає платформою для політичного діалогу з питань кібербезпеки. У рамках ООН діють робочі групи та комітети, що розробляють загальні принципи поведінки держав у кіберсфері. Зокрема, ухвалено резолюції Генасамблеї про кіберзлочинність і боротьбу з дезінформацією. Водночас через наявні розбіжності, зокрема між рф та західними країнами, процес формування міжнародних норм у сфері кібербезпеки залишається уповільненим, що ускладнює узгодження глобальних правил взаємодії в кіберпросторі. Попри це, ООН підтримує обмін досвідом і надає експертну допомогу державам, зокрема через програми Міжрегіональної консультативної групи ООН з кіберзлочинності та інші спеціалізовані ініціативи.

Північноатлантичний Альянс визначає протидію гібридним загрозам як один із ключових пріоритетів. НАТО розробило стратегію протидії гібридним загрозам та проводить спільні навчання, зокрема *NATO Cyber Coalition* та *Locked Shields*, спрямовані на відпрацювання реагування на кібератаки. За підтримки НАТО Україна реалізує проєкти, спрямовані на підвищення національної стійкості у сфері безпеки та оборони. З 2014 року функціонує Трастовий фонд НАТО з кібероборони для зміцнення української критичної інфраструктури. НАТО також активно співпрацює з країнами-партнерами. Альянс обмінюється розвідувальною інформацією про кіберзагрози та координує санкції. Дослідження показують, що НАТО визнає необхідність адаптувати свої стратегії проти дезінформації, пропаганди й кібератак. У рамках співпраці НАТО та ЄС у Спільній декларації 2018 р. сторони підтвердили обмін оперативною інформацією про кібератаки, посилення стійкості союзників та проведення узгоджених навчань.

ЄС розглядає гібридні атаки як загрозу демократичним цінностям і функціонуванню єдиного ринку. Європейська політика передбачає «м'який підхід» з фокусом на спільній роботі з державами-членами та партнерами. ЄС розвинув власні інституції: Європейське агентство кібербезпеки (ENISA) координує обмін даними між національними CERT, а Європейський Центр передового досвіду з протидії гібридним загрозам (Hybrid CoE) у Гельсінкі займається дослідженнями та тренінгами у галузі кібербезпеки й інформаційної гігієни. Єврокомісія запровадила Директиву NIS2, встановивши мінімальні вимоги до кібербезпеки критичної інфраструктури, та підтримує країни-союзники технічною допомогою. У партнерстві з НАТО ЄС спільно розробляє політики протидії дезінформації та кібератакам.

ОБСЄ спрямовує свої зусилля на побудову довіри між державами-учасницями в ІКТ-сфері. У 2013 р. ОБСЄ ухвалила Комплекс заходів з укріплення довіри для зниження ризиків конфліктів у зв'язку з використанням інформаційно-комунікаційних технологій. Ці заходи (СВМ) передбачають прозоре повідомлення про законодавчі й інституційні зміни у сфері кібербезпеки, обмін статистикою кіберінцидентів та контактних осіб для екстрених ситуацій. ОБСЄ проводить тренінги й консультації з кібергігієни та реагування на інциденти в межах ініціативи «Східне партнерство», що сприяє підвищенню компетентності країн регіону у сфері кібербезпеки [3].

Окрім глобальних організацій, особливе значення має регіональна координація. Так, у рамках Східного партнерства ЄС надає технічну допомогу Україні та іншим країнам Східної Європи у форматі спільних проєктів з кібербезпеки. Групи країн (наприклад "Трьох морів" у Європі) розвивають цифрову співпрацю. Важливі двосторонні ініціативи – наприклад, між Україною та США функціонують спільні військово-цифрові заходи: українські й американські експерти (команда Hunt Forward) спільно виявляють вразливості українських систем і підвищують їхній захист. За підсумками зустрічі у грудні 2024 р. сторони домовилися збільшити інвестиції у кіберінновації, посилити критичні комунікаційні мережі та впровадження ШІ. Подібно, Великобританія, Польща та країни Балтії активно діляться розвідданими з Україною та допомагають у розслідуванні російських кібератак.

Досвід України у протидії гібридній агресії отримав високу оцінку з боку міжнародних експертів. У відповідь на масштабні атаки 2014–2015 рр. держава запровадила комплексний підхід до посилення кібербезпеки: бкуло створено Цифровий оперативний штаб при Службі безпеки України та Центр протидії дезінформації, ухвалено Стратегію кібербезпеки (2016) та знизку аконодавчих ініціатив, зокрема щодо імплементації положень Директиви ЄС NIS2 та запровадження санкцій за кіберагресію. Зазначені кроки сприяли активнішій інтеграції України в європейські механізми кіберзахисту. Зокрема, українські фахівці Служби безпеки України пройшли навчання у країнах НАТО, а представники підрозділів зв'язку здійснюють обмін інформацією про реальні загрози з Естонською CERT. Водночас Україна виступає донором знань: напрацювання українських експертів, зокрема системи раннього виявлення інцидентів та моделі тренувань з протидії кібервійнам, упроваджуються партнерами. Очікувана перспектива членства України в НАТО та ЄС сприятиме подальшому прискоренню обміну інформацією й уніфікації стандартів кібербезпеки [4].

Міжнародне співробітництво має вирішальне значення для протидії гібридним загрозам та кібератакам. Світові організації ООН, НАТО, ЄС, ОБСЄ і регіони (Європа, Північна Америка, Азія) поступово створюють скоординований набір інструментів: від правових норм до технічних стандартів і оперативних каналів обміну. Приклади спільних ініціатив (трастові фонди, навчання, санкції, ЦОБМ ОБСЄ тощо) показують переваги злагоджених дій. Водночас виклики залишаються масштабними – від технологічного розриву до політичної

фрагментації. Таким чином, подальший розвиток механізмів співпраці, зокрема шляхом адаптації до новітніх технологій та розроблення уніфікованої нормативно-правової бази, є одним із пріоритетних напрямів забезпечення глобальної безпеки.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. С. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 09.10.2025).

2. Петік Я. Огляд засідань Відкритої робочої групи ООН з питань безпеки в кіберпросторі (2023). *Міжнародні відносини*. 2024. № 2 (59). С. 41–44.

3. Кацімон О. Україна та США посилюють співпрацю у сфері кібербезпеки та цифрових технологій. URL: https://ms.detector.media/trendi/post/36978/ (дата звернення 09.10.2025)

4. Спільна декларація про співпрацю ЄС і НАТО. Брюссель, 8 липня 2018 р. [Joint Declaration on EU-NATO Cooperation]. Офіц. вебсайт Ради ЄС. URL: https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf (дата звернення: 09.10.2025)