УДК 341.1/.8
DOI https://doi.org/10.32782/apdp.v103.2024.25

***О. І. Скіцько, Р. А. Ширшов***

# ДОСВІД КРАЇН-ЧЛЕНІВ НАТО З ОРГАНІЗАЦІЇ ТА ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРОБОРОНИ

**Постановка проблеми.** Повномасштабне вторгнення рф в Україну спричинило низку загроз світовій безпеці, з якими країни не стикалися раніше. Одночасно із безпосереднім веденням бойових дій та постійними силовими погрозами країнам Північноатлантичного Альянсу, країна агресор продовжує «гібридну війну», поєднуючи разом із застосуванням конвенційної зброї використання інших злочинних методів проти своїх противників – тероризм, кібервійна, торгові війни, підтримка реваншистських та сепаратистських рухів, пропаганда, порушення прав людини, злочини проти людяності, військові навчання, переселення, узурпація, вплив на громадську думку, злочинні акти цензури тощо [1]. Крім рф ще низка недружніх країн загрожують кібербезпеці НАТО. Причому в деяких з них, кібер-тероризм поставлений на «державну основу» як засіб політичного, економічного та військового впливу.

За даними сайту Statista, що є глобальною платформою даних і бізнес-аналітики, заснованою в Німеччині в 2007 році, у період з 2000 по 2023 роки у базі даних European Repository of Cyber Incidents (EuRepoC) було зафіксовано загалом 2506 політично вмотивованих кібератак у всьому світі. Ці кіберінциденти включають політизовані та неполітизовані атаки, спрямовані на політичні цілі, а також атаки на критичну інфраструктуру, незалежно від того, чи здійснюються вони державами (та афілійованими групами) або недержавними суб'єктами з політичними цілями.

Майже 12% політично вмотивованих кібератак, виявлених з початку століття, були здійснені з Китаю, за яким іде росія з подібною часткою (11,6%). Іран відповідальний за 5,3% цих кіберінцидентів за досліджуваний період, а Північна Корея – за 4,7%. Тут важливо зазначити, що більшість зловмисних дій цього типу (45%) не були належним чином розкриті, тобто країну походження в багатьох випадках неможливо було ідентифікувати. Майже третина проаналізованих політично вмотивованих кібератак була здійснена державами (або афілійованими групами) і така ж частка недержавними суб'єктами з політичними цілями. Близько половини зафіксованих атак були спрямовані на політичні цілі (громадські діячі, політичні партії тощо), а майже 20% – на об'єкти критичної інфраструктури [2].

Крім політичних та військових загроз, кібер-тероризм завдає значних економічних збитків країнам НАТО. Причому давно констатується, що деякі країни (зокрема, Північна Корея) розглядає кібератаки як бізнес, в тому числі. Згідно з оцінками Market Insights від Statista, очікується, що глобальні втрати від кіберзлочинності різко зростуть в наступні чотири роки з 9,22 трильйона доларів США у 2024 році до 13,82 трильйона доларів США до 2028 року.

**Аналіз останніх досліджень і публікацій.** Проблематику, пов'язану з вивченням досвіду країн – членів НАТО з організації та правового забезпечення кібероборони в своїх дослідженнях розглядали Гвоздь В., Горун О., Демедюк С., Завгородня Ю., Івасечко О., Кавин С., Користін О., Кулагін К., Мазулевський О., Поляков О., Слюсар В., Хівренко Д., Цебенко О., Чевардін В. та інші. Проте окремі аспекти досліджуваної проблематики залишились висвітлені не у повному обсязі.

**Метою статті** є розкриття особливостей нормативно-правового забезпечення та організації кібероборони в країнах – членах НАТО.

**Виклад основного матеріалу.** Сьогодні все більше і більше людей користуються Інтернетом, чи то для роботи, чи для особистого життя, а публічні відносини все більше переходять у цифровий простір, з'являється більше потенційних можливостей для кіберзлочинців. У той же час методи зловмисників стають все більш досконалими, з'являється більше інструментів для допомоги шахраям. Як пояснюють аналітики Statista Market Insights, пандемія коронавірусу призвела до того, що багато організацій зіткнулися з більшою кількістю кібератак через вразливість безпеки віддаленої роботи, а також через перехід до віртуалізованих ІТ-середовищ, таких як інфраструктура, дані та мережа хмарних обчислень. А повномасштабне вторгнення рф в Україну загострило зазначену проблематику.

Фахівці НАТО наголошують, що кіберзагрози безпеці Альянсу є «складними, руйнівними та насильницькими», і вони стають все більш частими. Кіберпростір завжди є предметом боротьби, і зловмисні кіберподії відбуваються щодня, від атак низького рівня до технологічно складних. НАТО та члени Альянсу у відповідь зміцнюють здатність Альянсу виявляти, запобігати та реагувати на зловмисну кібердіяльність. НАТО та її союзники покладаються на потужну та стійку систему кіберзахисту для виконання трьох основних завдань Альянсу: стримування та оборона, запобігання та врегулювання криз, а також спільна безпека. Альянс має бути готовим захистити свої мережі та операції від дедалі складніших кіберзагроз, з якими він стикається [3].

Від часу заснування НАТО кількість нових держав-членів альянсу збільшилася з первинних 12 до 32 країн. Останньою державою-членом, яка приєдналась до НАТО, стала Швеція – 7 березня 2024 року. НАТО зараз визнає Боснію і Герцеговину, яка отримала План дій щодо членства в НАТО в грудні 2018 року, Грузію та Україну як кандидатів на членство в альянсі. Також 19 інших держав беруть участь у програмі НАТО – Партнерство заради миру, ще 15 країн беруть участь в інституціоналізованих програмах діалогу.

Відповідно до статутних документів Альянсу головна роль НАТО полягає у забезпеченні свободи та безпеки країн-членів із використанням політичних і військових засобів. НАТО дотримується спільних для Альянсу цінностей демократії, індивідуальної свободи, верховенства права, мирного розв'язання суперечок і підтримує дані цінності в усьому євроатлантичному регіоні. Засадничим принципом Альянсу є спільність поглядів між північноамериканськими та європейськими членами НАТО, які поділяють однакові цінності та інтереси і віддані справі збереження демократичних принципів, що робить нероздільною безпеку Європи і Північної Америки. Альянс стоїть на захисті країн-членів від загрози агресії: голов-

ним військово-політичним принципом організації є система колективної безпеки, тобто спільних організованих дій усіх її членів у відповідь на напад ззовні [3].

НАТО як військово-політичний союз 32 держав є міжурядовою, а не наддержавною організацією. Це союз незалежних, суверенних держав, що об'єдналися в інтересах спільної безпеки та захисту спільних цінностей. Рішення в НАТО приймаються на основі консенсусу після обговорення і консультацій з країнами-членами Альянсу. Рішення, прийняте на основі консенсусу, є рішенням, згоду на яке дали і яке підтримали усі країни-члени Організації Північноатлантичного договору. Це означає, що рішення, прийняте НАТО, є виразом колективної волі суверенних держав, які є членами Альянсу. Принцип прийняття рішень на основі консенсусу стосується усіх справ Альянсу і віддзеркалює той факт, що рішення приймають саме країни-члени НАТО і кожна з них бере участь у процесі прийняття рішень. Цей принцип діє на усіх рівнях організації НАТО. У разі незгоди обговорення ведеться доти, доки рішення не буде прийняте, інколи це може призвести до визнання того, що досягти згоди неможливо. Але майже завжди вдається знайти взаємоприйнятне рішення. Консультації є невіддільною частиною процесу прийняття рішень в НАТО. Вони сприяють комунікації між країнами-членами, чиєю головною метою є прийняття таких колективних рішень, які відповідають їхнім національним інтересам [4].

Таким чином, розглядаючи правове регулювання країн – членів НАТО щодо безпекових питань, доцільно звернути увагу на правову базу самого Альянсу, тому що рішення НАТО приймаються на основі консенсусу учасників, а також враховуючи принцип верховенства міжнародного права над національним.

На теперішній час серед країн – членів НАТО діє угода про стандартизацію (STANAG), яка визначає процеси, процедури, терміни та умови спільних військових або технічних процедур для країн-членів альянсу. Кожна держава НАТО ратифікує STANAG і впроваджує його у своїх військових програмах. Мета STANAG полягає в тому, щоб забезпечити загальні оперативні і адміністративні процедури та матеріально-технічне забезпечення, щоб армія однієї країни-члена могла використовувати запаси та підтримку армії іншої країни-члена. STANAG також є основою для технічної сумісності між широким спектром комунікаційних та інформаційних систем (CIS), необхідних для операцій НАТО та Альянсу [5].

Згідно із документами НАТО, кіберзахист є частиною основного завдання НАТО зі стримування та оборони. У центрі уваги НАТО у сфері кібероборони – захист власних мереж, діяльність у кіберпросторі (зокрема через операції та місії Альянсу), допомога членам Альянсу у підвищенні їхньої національної стійкості та забезпечення платформи для політичних консультацій і колективних дій.

У липні 2016 року члени Альянсу підтвердили оборонний мандат НАТО та визнали кіберпростір областю операцій. НАТО служить платформою для політичних консультацій членів Альянсу, обміну занепокоєнням щодо зловмисної кіберактивності, обміну національними підходами та відповідями, а також розгляду можливих колективних заходів. Члени Альянсу зобов'язуються покращити обмін інформацією та взаємодопомогу у запобіганні, пом'якшенні наслідків, відновленні та реагуванні на кібератаки.

Члени Альянсу сприяють вільному, відкритому, мирному та безпечному кіберпростору та докладають зусиль для підвищення стабільності та зменшення ризику конфлікту, підтримуючи міжнародне право та добровільні норми відповідальної поведінки держав у кіберпросторі. У 2016 році члени Альянсу погодилися виконати зобов'язання щодо кіберзахисту. У 2023 році члени Альянсу посилили цю обіцянку та взяли на себе амбітні нові цілі щодо зміцнення національного кіберзахисту як пріоритетного питання, включно з критичною інфраструктурою. При цьому, на саміті НАТО 2021 року в Брюсселі члени Альянсу схвалили Комплексну політику кіберзахисту, яка підтримує три основні завдання НАТО, а також її загальну позицію стримування та оборони. Члени Альянсу підтвердили оборонний мандат НАТО та взяли на себе зобов'язання використовувати весь спектр можливостей для активного стримування, захисту та протидії повному спектру кіберзагроз у будь-який час, у тому числі шляхом розгляду колективної відповіді. Реагування має бути постійним і спиратися на елементи всього інструментарію НАТО, який включає політичні, дипломатичні та військові інструменти. Члени Альянсу також визнали, що вплив значної зловмисної сукупної кіберактивності за певних обставин може вважатися збройним нападом, який може змусити Північноатлантичну раду застосувати статтю 5 Північноатлантичного договору в кожному конкретному випадку. Альянс впевнений, що природа кіберпростору вимагає комплексного підходу через єдність зусиль на політичному, військовому та технічному рівнях.

На саміті НАТО у Вільнюсі 2023 року члени Альянсу схвалили нову концепцію посилення внеску кіберзахисту в загальну позицію стримування та оборони НАТО, а також розглянутий комплекс питань щодо кібероборони. Зокрема, стаття 66 Комюніке Вільнюського саміту зазначає, що суперництво у кіберпросторі є постійним, оскільки зловмисники дедалі частіше намагаються дестабілізувати Альянс за допомогою шкідливої кібердіяльності і кампаній. Загарбницька війна росії проти України висвітлила, наскільки кіберпростір став особливою характеристикою сучасного конфлікту.

Кіберзагрози, з якими стикаються країни – члени НАТО, є суттєвими, постійними і такими, що збільшуються. Лідери країн – учасників саміту заявили про свою рішучість використовувати увесь спектр спроможностей з метою стримування, захисту від і протидії повному переліку кіберзагроз, включаючи можливість запровадження колективних дій у відповідь на ці загрози. Важливою тезою є констатація, що окремі зловмисні кібернапади або їх сукупність можуть прирівнюватися до збройного нападу, внаслідок чого Північноатлантична рада може застосувати Статтю 5 Вашингтонського договору за відповідним рішенням у кожному конкретному випадку. Країни-учасники заявили про свою відданість зобов'язанням дотримуватися міжнародного права, включаючи Статут ООН, міжнародне гуманітарне право і міжнародне право у галузі прав людини в означених випадках. Альянс надалі сприятиме вільному, відкритому, мирному і безпечному кіберпростору і докладатиме зусиль для зміцнення стабільності і мінімізації ризику конфліктів, забезпечуючи дотримання міжнародного права і добровільні норми відповідальної поведінки держав у кіберпросторі.

Саміт затвердив нову концепцію піднесення ролі кіберзахисту у загальній позиції НАТО в галузі стримування і оборони. Завдяки їй буде краще інтегровано три рівні кіберзахисту НАТО – політичний, військовий і технічний – забезпечуючи постійне цивільно-військове співробітництво, як у мирний час, так і у разі криз і конфліктів, а також взаємодію з приватним сектором за доцільністю. Це допоможе поліпшити ситуаційну обізнаність Альянсу.

Посилення кіберстійкості Альянсу має вирішальне значення для зміцнення безпеки Альянсу і його здатності пом'якшувати значну шкоду, якої можуть потенційно завдавати кіберзагрози. Лідери країн-членів НАТО підтвердили зобов'язання Альянсу у сфері кібероборони та поставили на меті досягнення нових амбітних цілей на національному рівні щодо подальшого вдосконалення національного кіберзахисту держав – членів Альянсу як першочергового завдання, включаючи захист об'єктів критично важливої інфраструктури. Згаданий вище новий Віртуальний потенціал НАТО із забезпечення реагування на кіберінциденти (VCISC), який підкріплюватиме національні заходи, спрямований на пом'якшення наслідків у разі широкомасштабних зловмисних кібернападів. Завдяки цьому держави – члени Альянсу набувають додаткового інструменту надання та отримання допомоги [6].

Правову основу забезпечення кібероборони НАТО становить низка документів Альянсу, зокрема:

– Політика НАТО щодо кіберзахисту, схвалена міністрами оборони країн НАТО у червні 2011 року, в якій викладено бачення скоординованих зусиль у сфері кіберзахисту в усьому Альянсі в контексті загроз та технологічного середовища, що швидко змінюються;

– Політика кіберзахисту НАТО, схвалена на саміті НАТО в Уельсі 2014 року, у якій кіберзахист було визнано частиною основного завдання НАТО щодо колективної оборони. Це означає, що кібератака може бути підставою для застосування статті 5 установчого договору НАТО. Союзники також визнали, що в кіберпросторі застосовується міжнародне право;

– Технічна угода про кіберзахист між НАТО і ЄС, укладена в лютому 2016, метою якої є допомога обом організаціям краще запобігати кібератакам і реагувати на них;

– План дій з кіберзахисту (Cyber Defence Action), затверджений міністрами оборони країн Альянсу у лютому 2017 року разом із дорожньою картою впровадження кіберпростору як сфери операцій;

– Стратегічна концепція НАТО, ухвалена главами держав і урядів на Мадридському саміті НАТО 29 червня 2022 року;

– Нормативні положення з Комюніке Вільнюського саміту в частині кіберзахисту.

**Висновки.** Проблематиці кіберзахисту та кібероборони в цілому приділяється велика увага в нормативно-правових та стратегічних документах НАТО та країн-членів альянсу. Члени Альянсу неодноразово підтверджували оборонний мандат НАТО та взяли на себе зобов'язання використовувати весь спектр можливостей для активного стримування, захисту та протидії повному спектру кіберзагроз у будь-який час, у тому числі шляхом розгляду колективної відпо-

віді. Реагування має бути постійним і спиратися на елементи всього інструментарію НАТО, який включає політичні, дипломатичні та військові інструменти. Принципово важливим є визнання членами Альянсу того факту, що зловмисна кіберактивність за певних обставин може вважатися збройним нападом, який може змусити Північноатлантичну раду застосувати статтю 5 Північноатлантичного договору в кожному конкретному випадку. НАТО дійшло висновку, що природа кіберпростору вимагає комплексного підходу через єдність зусиль на політичному, військовому та технічному рівнях.

Усвідомлення цієї ситуації підсилюється кіберкампанією, яка є частиною нинішньої російської агресії проти України. Ця війна демонструє ставки у стратегічних змаганнях в кіберпросторі, де росія намагається пошкодити і розірвати українські військові, урядові і цивільні мережі і все, що від них залежить. Те, що росії досі не вдалося досягти стратегічного результату в Україні за допомогою кіберзасобів не означає, що потенційно вона не може цього зробити, і не повинно відволікати увагу від проблем, створюваних для воєнних зусиль України і потенціалу суспільства загалом це робити, через кібероперації російської військової розвідки.

Протягом багатьох років НАТО тісно співпрацює з Україною, щоб сприяти підвищенню її кіберзахисту. Кіберексперти НАТО в Брюсселі обмінюються інформацією зі своїми українськими колегами про поточну зловмисну кібердіяльність. Експерти Альянсу докладають багато зусиль для підтримки фахівців в Україні. НАТО і Україна мають низку угод про посилене кібернетичне співробітництво, включаючи доступ України до платформи обміну інформацією НАТО про шкідливі програми. У 2023 році Україна офіційно приєдналася до Центру НАТО з питань співробітництва в галузі кіберзахисту.

### *Література*

1. Daniel T. Lasica. Strategic Implications of Hybrid War: A Theory of Victory – War College Series. Bibliolife DBA of Bibilio Bazaar II LLC, 2015. 66 p.

2. Fleck A. Who's Behind Cyber Attacks? URL : https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/.

3. Офіційний сайт НАТО. URL: https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en

4. Office of Information and Press NATO – 1110 Brussels – Belgium. 2001. URL: https://www.nato.int/docu/other/ukr/handbook/2001/pdf/handbook.pdf

5. NATO Interoperability Standards and Profiles. Стандарти та профілі оперативної сумісності НАТО. 2023. https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/volume1/index.html

6. Комюніке Вільнюського саміту НАТО : Вільнюс 11 лип. 2023 року. URL : https://www.nato.int/cps/ru/natohq/official_texts_217320.htm?selectedLocale=uk

## Анотація

***Скіцько О. І., Ширшов Р. А.*** **Досвід країн-членів НАТО з організації та правового регулювання кібероборони.** – Стаття.

Сьогодні дедалі частішими стають кіберзагрози безпеці Альянсу. Суперництво у кіберпросторі є постійним, оскільки зловмисники дедалі частіше намагаються дестабілізувати Альянс за допомогою шкідливої кібердіяльності і кампаній. У відповідь на це НАТО та члени Альянсу зміцнюють його здатність виявляти, запобігати та реагувати на зловмисну кібердіяльність. У минулому році члени Альянсу взяли на себе цілі щодо зміцнення національного кіберзахисту як пріоритетного питання та схвалили нову концепцію посилення внеску кіберзахисту в загальну позицію стримування та оборони НАТО. Відповідно до нормативно-правової бази Альянсу дає можливість прирівнювати окремі зловмисні кібернапади або їх сукупність до збройного нападу, внаслідок чого Північноатлантична рада може застосувати Статтю 5 Вашингтонського договору за відповідним рішенням у кожному конкретному випадку.

У відповідних правових нормах Альянсом було закріплено принципову позицію щодо подальшого сприяння вільному, відкритому, мирному і безпечному кіберпростору, а також зобов'язання щодо зміцнення стабільності і мінімізації ризику конфліктів, забезпечуючи дотримання міжнародного права і добровільні норми відповідальної поведінки держав у кіберпросторі. Саміт затвердив нову концепцію піднесення ролі кіберзахисту у загальній позиції НАТО в галузі стримування і оборони, завдяки чому буде краще інтегровано три рівні кіберзахисту НАТО – політичний, військовий і технічний. Такий підхід забезпечить постійне цивільно-військове співробітництво, як у мирний час, так і у разі криз і конфліктів, а також взаємодію з приватним сектором за доцільністю, що допоможе поліпшити ситуаційну обізнаність Альянсу. Члени Альянсу неодноразово підтверджували оборонний мандат НАТО та взяли на себе зобов'язання використовувати весь спектр можливостей для активного стримування, захисту та протидії повному спектру кіберзагроз у будь-який час, у тому числі шляхом розгляду колективної відповіді. Реагування має бути постійним і спиратися на елементи всього інструментарію НАТО, який включає політичні, дипломатичні та військові інструменти.

*Ключові слова:* кіберзагрози, кібероборона, кіберінцедент, кіберпростір, кібернапад.

## Summary

***Skitsko O. I., Shirshov R. A.*** **Experience of NATO member countries in the organization and legal regulation of cyber defense.** – Article.

Today, cyber threats to the security of the Alliance are becoming more frequent. Rivalry in cyberspace is constant as attackers increasingly seek to destabilize the Alliance through malicious cyber activities and campaigns. In response, NATO and Allies are strengthening its ability to detect, prevent and respond to malicious cyber activity. Last year, Allies committed to strengthening national cyber defense as a priority and approved a new concept for strengthening the contribution of cyber defense to NATO's overall deterrence and defense posture. According to the normative and legal framework of the Alliance, it is possible to equate individual malicious cyber attacks or their combination with an armed attack, as a result of which the North Atlantic Council can apply Article 5 of the Washington Treaty on a case-by-case basis.

In the relevant legal regulations, the Alliance established a principled position on the further promotion of a free, open, peaceful and safe cyberspace, as well as obligations to strengthen stability and minimize the risk of conflicts, ensuring compliance with international law and voluntary norms of responsible behavior of states in cyberspace. The summit approved a new concept of elevating the role of cyber defense in NATO's overall deterrence and defense posture, thanks to which the three levels of NATO cyber defense – political, military and technical – will be better integrated. This approach will ensure ongoing civil-military cooperation, both in peacetime and in the event of crises and conflicts, as well as interaction with the private sector as appropriate, which will help improve the Alliance's situational awareness. Alliance members have repeatedly reaffirmed NATO's defense mandate and committed to using the full range of capabilities to proactively deter, protect and counter the full range of cyber threats at all times, including through consideration of a collective response. The response must be sustained and draw on elements of the entire NATO toolkit, which includes political, diplomatic and military instruments.

*Key words:* cyber threats, cyber defense, cyber incident, cyberspace, cyber attack.