NATO's approach to space. (2019). *NATO official website.* Retrieved from https://www.nato.int/cps/en/natohq/topics_175419.htm
Deterrence and defence. (2020). *NATO official website.* Retrieved from https://www.nato.int/cps/en/natohq/topics_133127.htm
A «comprehensive approach» to crises. (2021). *NATO official website.* Retrieved from https://www.nato.int/cps/en/natohq/topics_51633.htm
NATO Warfighting Capstone Concept. (2021). *NATO official website.* Retrieved from https://www.act.nato.int/our-work/nato-warfighting-capstone-concept/
NATO 2022 Strategic Concept. (2022). *NATO official website.* Retrieved from https://www.nato.int/cps/en/natohq/topics_210907.htm
NATO Integrated Air and Missile Defence Policy. (2025). *NATO official website.* Retrieved from https://www.nato.int/cps/en/natohq/official_texts_233084.htm

Анастасія САДОМОВА
студентка кафедри міжнародних відносин і аудиту
НТУ «Дніпровська політехніка»
Науковий керівник - к.і.н., с.н.с, Тетяна КУЛИК

ПОЛІТИКА НАТО З КІБЕРБЕЗПЕКИ: МЕТОДИ ТА ВИКЛИКИ

У XXI столітті кіберпростір став ключовою складовою безпекового середовища. Інформаційна безпека зазнає суттєвих трансформацій через розвиток технологій, появу нових викликів і загроз, а також через зміни у значенні інформації в сучасному світі. Зростання кількості кібератак на державні інституції, інфраструктуру та інформаційний простір, а також активне використання дезінформації й кібероперацій у гібридних конфліктах зумовлюють нагальну потребу формування ефективної політики кіберзахисту. Нині інформаційна сфера стала важливою частиною стратегічного планування міжнародних організацій, які формують стратегії та спільні заходи, спрямовані на протидію загрозам у сфері інформаційної та кібернетичної безпеки. НАТО як організація колективної оборони та одна з найвпливовіших міжнародних структур, відіграє ключову роль у формуванні глобальної архітектури безпеки в кіберпросторі, базуючи свій підхід до протидії викликам на демократичних принципах та нормах міжнародного права.

Для України, яка перебуває в умовах широкомасштабної агресії, питання кібербезпеки набуває особливого значення, з огляду на численні атаки на об'єкти критичної інфраструктури, урядові сайти, енергосистему, інформаційну сферу. У цьому контексті досвід і політика НАТО, як провідного оборонного альянсу, є надзвичайно важливими як практичний орієнтир у рамках партнерства. Зокрема, участь України в Платформі розширених можливостей НАТО (Enhanced

Opportunities Partnership) відкриває доступ до обміну досвідом, навчань і оперативної взаємодії в кіберсфері (Relations, 2025).

Метою даного дослідження є аналіз трансформації підходів НАТО у сфері кібербезпеки протягом 2002–2024 років, виявлення ключових методів забезпечення кіберзахисту, а також визначення викликів та перспектив подальшого розвитку політики Альянсу.

Політика кібербезпеки НАТО почала формуватись після ухвалення Празької декларації (2002), однак імпульс до її активного розвитку надала кібератака на Естонію у 2007 році, після якої Альянс визнав потребу у посиленому реагуванні на кіберзагрози. У 2008 р. було створено Центр передового досвіду з кібероборони в Таллінні (CCDCOE), а в 2016 році на Варшавському саміті кіберпростір було офіційно визнано окремим операційним доменом поряд із сушею, морем, повітрям і космосом (Cyber, 2016). Це не означає, що кіберпростір став територією застосування збройної сили, однак він розглядається як середовище, у якому Альянс може здійснювати оборонні операції, включно з підтримкою колективного захисту згідно зі статтею 5. Згідно з запровадженою ініціативою Cyber Defence Pledge (2016), країни-члени зобов’язалися модернізувати свої спроможності, адаптувати національні стратегії та забезпечити взаємну сумісність (Cyber, 2016).

У 2021 році на зустрічі в Брюсселі НАТО ухвалило комплексну стратегію кібербезпеки для підтримки ключових завдань Альянсу. Стратегія підкреслює оборонну місію організації та зобов'язання протидіяти кіберзагрозам через створення спільних механізмів реагування та використання всіх доступних політичних, дипломатичних та військових інструментів. Підхід базується на трьох принципах: стримування, захист та реагування. Альянс працює над забезпеченням вільного, відкритого та безпечного кіберпростору, зміцненням стабільності та підтримкою відповідальної поведінки держав у віртуальному просторі (Brussels, 2021).

У червні 2022 року НАТО затвердило нову Стратегічну концепцію, яка визначила головне призначення Альянсу як забезпечення колективної оборони на основі спільних цінностей - свободи, прав людини, демократії та верховенства права. Росію визнано найбільшою прямою загрозою через її агресивну політику та використання військових, кібер та гібридних методів. Вперше увагу приділено Китаю як серйозному виклику через нарощування глобальної присутності. На саміті у Вільнюсі 2023 року союзники затвердили нову стратегію підвищення ролі кіберзахисту, посилили зобов'язання щодо захисту критичної інфраструктури та запустили Віртуальний центр підтримки у випадку кіберінцидентів (VCISC) (Vilnius, 2023).

У 2023–2024 рр. кіберпростір залишився пріоритетним напрямом діяльності, що зафіксовано у звітах Генерального секретаря та у підсумках Вільнюського саміту (Vilnius, 2023b). Зокрема, Звіт констатує, що «кіберпростір став постійною ареною протистояння, де зловмисні дії стратегічних суперників

загрожують демократичним системам і критичній інфраструктурі. Війна росії проти України підтвердила роль кіберзагроз у сучасних конфліктах. НАТО використовує повний спектр інструментів для стримування та захисту, просуваючи принципи безпечного та стабільного кіберпростору на основі міжнародного права» (NATO, 2024).

НАТО протидіє інформаційним загрозам через комплексну співпрацю з національними урядами держав-членів, країн-партнерів та міжнародними організаціями, включаючи ЄС, G7, ООН та ОЕСР. Альянс також працює з приватними компаніями, медіаорганізаціями, соціальними платформами, громадськими організаціями та науковими установами для вивчення загроз і розробки стратегій протидії. Важливим елементом боротьби є превентивне поширення достовірної інформації через відкриті комунікації з громадськістю, що дозволяє завчасно нейтралізувати загрози та випереджати ворожі наративи. НАТО використовує соціальні мережі, зв'язки з медіа та вебсторінку. Група швидкого реагування НАТО створює експертні мережі, забезпечує раннє попередження про інформаційні загрози та гарантує здатність швидкого реагування (NATO, 2025).

На Вашингтонському саміті 2024 року було створено Інтегрований центр кіберзахисту Альянсу для зміцнення захисту мереж і впровадження кіберпростору як повноцінної операційної сфери НАТО. Ключові завдання включають централізований захист мереж, ефективний моніторинг кіберзагроз, інтеграцію кіберпростору в загальну оборонну стратегію, протидію гібридним загрозам з боку Росії та Китаю, а також розвиток співпраці з ЄС у сфері кібербезпеки (Washington, 2024).

Політика кібербезпеки НАТО є багатовимірною та постійно адаптується до змін середовища, у якому зростають як масштаби, так і складність кіберзагроз. Альянс усвідомив, що кіберзагрози більше не є другорядними — вони перетворилися на повноцінні інструменти гібридної війни, здатні порушити стабільність держав, спричинити економічні збитки та підірвати довіру до демократичних інституцій. НАТО визнало кіберпростір окремою сферою ведення війни, що дозволило включити кібернетичні дії в загальну військову стратегію. Альянс активно залучає не лише державні структури, а й приватні технологічні компанії, наукові установи, громадянське суспільство та медіаплатформи. Такий підхід забезпечує оперативний доступ до передових технологій, сприяє інноваціям та дозволяє виявляти і нейтралізувати загрози ще до їхнього масштабування. Превентивна інформаційна політика, заснована на прозорій комунікації з громадськістю, запобігає поширенню дезінформації та протидіє ворожим наративам на етапі їх формування.

НАТО не створює спільних юридичних правил з ЄС, оскільки обидві організації не мають законодавчого мандату одна щодо одної. Проте між ними активно розвивається координація зусиль, яка передбачає обмін інформацією, спільні навчання та стандарти безпеки. Цей підхід закріплено у Третьому

спільному комюніке НАТО-ЄС 2023 (Joint, 2023).

Водночас Альянс стикається з низкою серйозних викликів. Хакерські атаки стали більш координованими і технологічно витонченими, що значно ускладнює їхнє своєчасне виявлення та нейтралізацію. Особливої уваги заслуговує гібридний характер загроз, де кіберзасоби поєднуються з дезінформацією, спрямованою на підрив довіри до демократичних інституцій. Серйозною загрозою залишається державне спонсорування кібероперацій з боку авторитарних режимів - Російська Федерація ідентифікована як головна пряма загроза безпеці держав-членів, а Китай — як довгостроковий системний виклик. Ці країни активно використовують кіберпростір як інструмент геополітичного впливу, від кібер-шпигунства до втручання у внутрішні справи інших держав. Додатковим ризиком є технологічна конкуренція та виклики нових технологій, які створюють як можливості, так і загрози для кіберстійкості Альянсу (НАТО, 2022).

Аналіз політики НАТО в кіберсфері засвідчує її багаторівневу структуру, водночас виявляє внутрішні суперечності. Сильні сторони політики Альянсу пов'язані з її інституційною стабільністю та координаційним потенціалом. По-перше, НАТО володіє спеціалізованими структурами, такими як Cyber Defence Committee та CCDCOE, які забезпечують постійну експертну підтримку. По-друге, здатність до оперативної мобілізації підтверджується регулярними навчаннями (*Locked Shields*, *Cyber Coalition*), у яких беруть участь країни-члени й партнери (Locked, 2023). По-третє, інтеграція партнерів (зокрема України, Фінляндії, Швеції) у кіберініціативи посилює ефективність колективної відповіді.

Водночас слабкі сторони полягають у фрагментарності національних підходів, оскільки кожна країна-член самостійно забезпечує кіберзахист, що ускладнює гармонізацію реагування. Крім того, відсутність чіткого визначення умов застосування статті 5 у випадку кіберінциденту створює ситуацію правової невизначеності (Robinson, 2016). Як відзначають фахівці, ефективність кіберполітики НАТО значною мірою залежить не лише від технологічного оснащення, але й від політичної здатності країн-членів узгоджувати свої інтереси та оперативно реагувати в умовах кризи (Karatas, 2021).

Ще одним викликом є еволюція противників. Росія, Китай та інші авторитарні актори дедалі частіше використовують методи обману, маніпуляції, атак через третіх осіб, що ускладнює атрибуцію ключовий елемент колективної відповіді НАТО (Morgan, 2024).

Для подальшого зміцнення позицій у сфері інформаційної безпеки, НАТО має прискорити створення нового центру кіберзахисту та впровадити технології штучного інтелекту для раннього виявлення загроз.

Аналіз еволюції політики кібербезпеки НАТО з 2002 по 2024 рік свідчить значну трансформацію від початкового усвідомлення проблеми до створення комплексної системи кіберзахисту. Альянс пройшов шлях від обговорення

загроз у 2002 році до визнання кіберпростору повноцінною операційною сферою та створення спеціалізованих центрів. НАТО розробила багатовимірний підхід протидії кіберзагрозам, заснований на принципах стримування, захисту та реагування через комплексну співпрацю з державними структурами, приватними компаніями та міжнародними організаціями, превентивне поширення достовірної інформації та використання всіх доступних політичних, дипломатичних та військових інструментів. Незважаючи на серйозні виклики у сфері кібербезпеки, еволюція політики НАТО демонструє успішну адаптацію до змінюваного середовища кіберзагроз та трансформацію розуміння кіберпростору від технічної проблеми до критично важливої сфери оборони.

З урахуванням наведеного аналізу, перспективи розвитку кіберполітики НАТО полягають у трьох взаємопов'язаних напрямах, таких як технологічна інтеграція, нормативна конкретизація та партнерська кооперація з Україною. Альянсу необхідно впроваджувати нові підходи до виявлення загроз, зокрема використання штучного інтелекту для виявлення аномалій і поведінкових моделей атак. Крім того, потенційне створення спільного оперативного центру з використанням AI-аналізу даних сприятиме зниженню часу реагування на кіберінциденти. Також, потрібна розробка умов, за яких кібератака може трактуватись як casus belli, з подальшим застосуванням колективних заходів. Це дозволить уникнути правової невизначеності в разі серйозної ескалації.

Розширення участі України в спільних кібернавчаннях, надання доступу до обмежених мережевих платформ спільного попередження, а також залучення українських фахівців до розробки кейсів гібридних сценаріїв зміцнить стійкість східного флангу Альянсу та сприятиме технологічному обміну. Узгодження цих напрямів створює основу для стійкого та адаптивного кіберзахисту як НАТО, так і країн-партнерів, насамперед України.

Список використаних джерел

Brussels Summit Communiqué. (2021). Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council/ *NATO official website*. Retrieved from: https://www.nato.int/cps/en/natohq/news_185000.htm

Cyber defence. (Jul. 2024). *NATO official website*. Retrieved from: https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en

Cyber Defence Pledge (2016). *NATO official website*. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Joint Declaration on EU-NATO Cooperation. (2023). *NATO official website*. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_210549.htm

Karatas, I. (2021). Cyber Warfare and NATO's New Security Concept: Smart Defense. *NATO and the Future of European and Asian Security.* Retrieved from:
https://www.academia.edu/71039100/Chapter_Cyber_Warfare_and_NATOs_New_Security_Concept_Smart_Defense

Locked Shields 2023 Wrap-Up CCDCOE. (2023). *NATO Cooperative Cyber Defence Centre of Excellence*. Retrieved from: https://ccdcoe.org

Morgan, E. (2024). Eroding Global Stability: The Cybersecurity Strategies Of China, Russia, North Korea, And Iran. *Irregular Warfare Initiative*. Retrieved from: https://irregularwarfare.org/articles/eroding-global-stability-the-cybersecurity-strategies-of-china-russia-north-korea-and-iran/

NATO 2022 Strategic Concept. (2022). Adopted by Heads of State and Government at the NATO Summit. *NATO official website*. Retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO's approach to counter information threats. (2025). *NATO official website*. Retrieved from: https://www.nato.int/cps/uk/natohq/topics_219728.htm?SelectedLocale=en

NATO Secretary General's Annual Report 2023. (Mar. 2024). *NATO official website*. Retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/3/pdf/sgar23-en.pdf

Relations with Ukraine. Mar. (2025). *NATO official website*. Retrieved from: https://www.nato.int/cps/en/natohq/topics_37750.htm?selectedLocale=en

Robinson, N. (2016). NATO: changing gear on cyber defence. *NATO Review.* Retrieved from: https://www.nato.int/docu/review/articles/2016/06/08/nato-changing-gear-on-cyber-defence/index.html

Vilnius Summit Communiqué. (2023). *NATO official website*. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_217320.htm?selectedLocale=en

Washington Summit Declaration. (2024). *NATO official website*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_227678.htm?selectedLocale=en

Брежнєва Т.В. (2012). Політика НАТО з кіберзахисту та співробітництво з партнерами. *Стратегічні пріоритети.* № 4. СС.189-194.