УДК 327.5
DOI: 10.24144/2078-1431.2025.1(34).69-79

Оксана Фролова,
кандидат політичних наук,
доцент кафедри міжнародної інформації
Навчально-наукового інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка
ORCID ID: 0000-0001-7105-2762

Валерія Теренник,
студентка 2 курсу магістратури
спеціальності «Міжнародні комунікації»
Навчально-наукового інституту міжнародних відносин
Київського національного університету імені Тараса Шевченка

СПІВРОБІТНИЦТВО МІЖ УКРАЇНОЮ ТА НАТО У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Співробітництво України та НАТО у сфері інформаційної безпеки є важливим елементом зміцнення стійкості держави до гібридних загроз. У статті аналізуються основні напрями взаємодії, зокрема Комплексний пакет допомоги (CAP), співпраця з CCDCOE, створення JATEC, а також заходи з протидії дезінформації та кіберзагрозам. Досліджено механізми інтеграції України в євроатлантичний кіберпростір, розглянуто основні виклики та перспективи подальшого розвитку стратегічної співпраці у сфері кібербезпеки та інформаційної протидії.

Ключові слова: *гібридні загрози, стратегічна комунікація, кібербезпека, національна безпека, дезінформація, євроатлантична інтеграція, інформаційна стійкість.*

The article examines the challenges of Ukraine's information security in the context of hybrid warfare and explores NATO-Ukraine cooperation mechanisms in this domain. The study identifies key threats, including large-scale cyberattacks, disinformation campaigns, and election interference, which significantly impact Ukraine's national security. The research is based on an analytical approach, including case studies of Russian cyber operations and disinformation tactics.

The findings highlight NATO's role in strengthening Ukraine's resilience through strategic initiatives such as the Comprehensive Assistance Package (CAP), cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), and the establishment of the Joint Analysis, Training, and Education Centre (JATEC). These mechanisms enable Ukraine to integrate into the Euro-Atlantic security framework, enhancing cyber defense capabilities, intelligence sharing, and strategic communications.

Despite significant progress in cybersecurity and countering disinformation, challenges remain, including the need for institutional reforms, technological advancements, and deeper coordination with NATO allies. The study concludes that Ukraine's

long-term security strategy must focus on further strengthening digital resilience, expanding international cooperation, and developing rapid response mechanisms to hybrid threats. The creation of JATEC marks a significant milestone in Ukraine-NATO relations, reinforcing Ukraine's role as a key security partner of the Alliance.

***Keywords**: hybrid threats, strategic communication, cybersecurity, national security, disinformation, Euro-Atlantic integration, information resilience.*

Сучасні інформаційні загрози займають центральне місце у гібридній війні, спрямованій на дестабілізацію суспільств та підрив довіри до державних інституцій. У контексті збройної агресії РФ особливої ролі набуває співробітництво України з НАТО для підвищення стійкості до інформаційних загроз.

Гібридна війна включає широкий спектр інформаційних операцій, спрямованих на підрив демократичних інститутів, викривлення реальності та поширення хаосу в суспільстві. РФ використовує Україну як полігон для випробовування нових методів і засобів ведення гібридної війни. Так, однією із загроз є масові кібератаки на критичну інфраструктуру, які стали серйозною проблемою для України. Кібератаки на енергосистему, банківську сферу та державні органи призводять до масштабних економічних втрат та дестабілізації роботи державних установ [14]. Одночасно з цим дуже частим інструментом, який використовує РФ, є дезінформаційні кампанії. Так, Росія використовує соціальні мережі та підконтрольні медіа для поширення маніпулятивних наративів, спрямованих на дискредитацію української влади та підрив підтримки міжнародних партнерів. Одним із найбільш відомих прикладів є кампанія щодо дискредитації українських військових через неправдиві звинувачення у військових злочинах, які поширювалися відразу на декількох платформах.

Втручання у виборчі процеси є ще одним важливим аспектом інформаційної війни: використання ботоферм та фабрик тролів для маніпуляції громадською думкою під час президентських та місцевих виборів демонструє активні спроби Росії впливати на внутрішньополітичні процеси в Україні [14]. Наприклад, під час президентських виборів 2019 року було зафіксовано численні дезінформаційні кампанії, які поширювалися через російські пропагандистські сайти, такі, як «NewsFront» та «Звезда», а також через різні Telegram-канали [10]. Тут також варто відмітити високий рівень адаптивності РФ, адже вже зараз вона використовує «викривлене» втручання у виборчі процеси, застосовуючи дезінформаційні кампанії, спрямовані на підрив легітимності української влади та дестабілізацію політичної ситуації в країні. Зокрема, у 2024 році була зафіксована кампанія під назвою «Майдан-3», яка ставила під сумнів легітимність рішень української влади після 20 травня 2024 року, намагаючись спровокувати панічні настрої та дискредитувати Президента України перед міжнародними партнерами [2].

Крім того, російські хакери неодноразово здійснювали кібератаки, спрямовані на підрив інформаційної безпеки України. Так, у січні 2022 року вони атакували близько 70 державних вебсайтів, зокрема сторінки

Міноборони, МЗС, ДСНС та інших відомств, залишаючи погрозливі повідомлення українською, російською та польською мовами. Одразу після цього у даркнеті з'явилося оголошення про продаж 30 ГБ персональних даних понад двох мільйонів українців, які нібито були викрадені з порталу «Дія». Російські інформаційні ресурси та проросійські Telegram-канали активно розкручували цей наратив, намагаючись підірвати довіру до цифрових державних сервісів України. Проте Міністерство цифрової трансформації України та незалежні експерти з кібербезпеки встановили, що дані були скомпільовані з різних джерел і не мали жодного стосунку до реальних реєстрів «Дії». Подібні інформаційно-психологічні операції є типовими інструментами гібридної війни, які Росія використовує для створення хаосу та недовіри всередині українського суспільства [15].

Росія також часто використовує проксі-ЗМІ та маргінальні медіа, що поширюють вигідні Росії наративи, спрямовані на розпалювання паніки, підрив морального духу населення та загальну дестабілізацію суспільного порядку. Одним із яскравих прикладів є діяльність медіакомпаній RT та Sputnik, які, будучи фінансованими державою, поширюють провладні наративи на міжнародну аудиторію [12]. Крім того, тут варто згадати і про мережу Pravda, сайти і телеграм-канали якої «публікують дискредитаційні, маніпулятивні та фейкові матеріали щодо подій, які будь-яким чином стосуються України, зокрема російсько-української війни» [2].

Останньою загрозою, про яку ми тут згадаємо, є використання сучасних технологій, таких, як deepfake та штучний інтелект, які значно ускладнюють ідентифікацію фальсифікованого контенту. Відео та аудіозаписи, створені за допомогою штучного інтелекту, здатні дискредитувати політичних та військових лідерів України, що особливо небезпечно у кризові періоди [3]. Наприклад, у вересні 2024 року голова Комітету з міжнародних відносин Сенату США Бен Кардін став жертвою deepfake-дзвінка, під час якого зловмисник видавав себе за тодішнього міністра закордонних справ України Дмитра Кулебу. Цей інцидент підкреслює зростаючу загрозу використання технологій deepfake для політичних маніпуляцій та дезінформації [17].

Як бачимо, Україна стикається з великою кількість загроз в інформаційній сфері, тож подальше зміцнення міжнародного партнерства є критично важливим. Наразі НАТО та країни-члени Альянсу відіграють ключову роль у наданні технологічної та методологічної підтримки Україні, що, в свою чергу, дозволяє ефективно протистояти сучасним інформаційним викликам. Розширення кіберспроможностей, обмін аналітичними даними та посилення стратегічних комунікацій є необхідними кроками для підвищення рівня інформаційної безпеки [23].

Співробітництво між Україною та НАТО у сфері інформаційної безпеки базується на розгалуженій інституційній структурі та ефективних механізмах взаємодії, спрямованих на протидію сучасним інформаційним загрозам та зміцненні кібербезпеки. *Комплексний пакет допомоги НАТО (CAP)* став ключовим механізмом підтримки України у сфері безпеки та оборони. Його було запроваджено у 2016 році на Варшавському саміті як

відповідь на незаконну анексію Криму та агресію Росії на Донбасі, а у 2022 році — значно розширено під час Мадридського саміту, після початку повномасштабного російського вторгнення. CAP охоплює два основні напрями: короткострокову нелетальну військову допомогу (постачання медичного обладнання, засобів зв'язку, систем захисту та розмінування) та довгострокові програми з розбудови спроможностей, які включають реформування сектору безпеки, кібероборону, боротьбу з дезінформацією та підвищення оперативної сумісності з НАТО [16]. Завдяки оновленому CAP, остаточно ухваленому на Вільнюському саміті 2023 року, допомога Україні отримала багаторічний характер із передбачуваним фінансуванням. У сфері кіберзахисту та інформаційної безпеки CAP передбачає посилену технічну підтримку, інтеграцію України в євроатлантичний кіберпростір, впровадження передових технологій захисту критичних інформаційних систем та розвиток спроможностей протидії гібридним загрозам [20]. Зокрема, Україна отримала доступ до новітніх засобів кібероборони, зокрема в межах співпраці з *Об'єднаним центром передових технологій з кібероборони НАТО (CCDCOE),* розташованим у Таллінні. Цей центр є провідною структурою Альянсу у сфері кібероборони, що забезпечує стратегічний аналіз, дослідження та навчання для держав-членів і партнерів. Процес приєднання України розпочався у 2021 році, коли Національний координаційний центр кібербезпеки при РНБО подав офіційний запит. Після схвалення заявки всіма країнами-учасницями у 2022 році у травні 2023 року Україна стала повноправним членом CCDCOE. Це дозволило українським фахівцям брати участь у міжнародних дослідженнях, отримувати доступ до аналітичних даних щодо новітніх кіберзагроз та долучатися до розробки спільних політик кібероборони в рамках НАТО [9]. Так, завдяки цій співпраці, Україна мала змогу взяти участь у міжнародних кібернавчаннях, таких, як «Locked Shields» — найбільші у світі навчання з кібербезпеки, які імітують реальні загрози для критичної інфраструктури. У 2024 році Україна вперше взяла в них участь як повноправний член НАТО CCDCOE, працюючи спільно з Чехією. Ці навчання передбачають не лише технічні сценарії відбиття атак, а й стратегічне планування, комунікації в кризових ситуаціях та правові аспекти кібероборони [5]. Попередньо Україна брала участь у навчаннях «Cyber Coalition», які є найбільшими щорічними тренуваннями Альянсу у сфері кіберзахисту, під час яких учасники відпрацьовують сценарії реагування на загрози, що включають атаки на критичну інфраструктуру, системи енергопостачання та військові комунікації [6]. Тож, як бачимо, взаємодія з CCDCOE сприяє інтеграції України в єдину систему кібероборони НАТО, посиленню її стійкості до кібератак та підвищенню професійного рівня українських фахівців у сфері кібербезпеки.

НАТО також підтримує Україну через *Цільовий фонд CAP*, до якого з 2022 року союзники та партнери спрямували майже 800 мільйонів євро. Ці кошти використовуються для забезпечення захисту критичної інфраструктури, кібербезпеки, розмінування, медичної реабілітації військових, а також удосконалення оборонних закупівель відповідно до стандар-

тів НАТО. Комплексний пакет допомоги відіграє важливу роль у трансформації інформаційного безпекового сектору України, наближаючи її до взаємосумісності з НАТО [20]. Окрім цього, НАТО також підтримує Україну через *Трастовий фонд з кібербезпеки*, що спрямований на створення національних груп реагування на кіберінциденти (CSIRT) та розвиток захисних технологій. У рамках цього фонду відбувається модернізація кіберінфраструктури державного сектору, впровадження механізмів раннього виявлення кібератак та розробка політик кіберзахисту [23].

У межах Комплексного пакету допомоги також існує *Платформа Україна — НАТО з протидії гібридній війні*, яка є одним з ключових механізмів протидії гібридним загрозам, зокрема інформаційним і кібернетичним атакам. Платформа була заснована в 2016 році з метою виявлення та аналізу гібридних загроз, посилення національної стійкості, а також впровадження заходів щодо їхньої нейтралізації [22]. Ця ініціатива передбачає обмін досвідом між Україною та країнами-членами Альянсу, дослідження нових методів інформаційної боротьби та координацію заходів у сфері кіберзахисту, стратегічних комунікацій і безпеки критичної інфраструктури. В межах Платформи реалізовано низку ініціатив, серед яких особливу увагу приділено впровадженню стратегічних комунікацій, розбудові системи раннього виявлення інформаційних загроз та зміцненню національних можливостей у сфері кібербезпеки. Також Платформа відіграє важливу роль у розробці протоколів швидкого реагування на інформаційні атаки, які можуть впливати на політичну та соціальну стабільність країни. Крім того, значні зусилля спрямовані на аналіз російських дезінформаційних кампаній, які поширюються через соціальні мережі та проросійські медіа, що дозволяє краще прогнозувати та нейтралізувати загрози інформаційного характеру [14]. В умовах повномасштабної агресії Росії діяльність Платформи активізувалася, зокрема через регулярні консультації, навчання та спільні ініціативи. Так, у листопаді 2023 року в Кишиневі відбулася зустріч представників України, НАТО та ЄС, присвячена аналізу новітніх гібридних загроз та розширенню міжвідомчої співпраці. Особливу увагу приділили стратегічним комунікаціям, протидії дезінформації, енергетичній безпеці та захисту критичної інфраструктури. Співпраця в межах Платформи сприяє розбудові стійких механізмів запобігання та реагування на інформаційні атаки, що є важливим елементом євроатлантичної інтеграції України та зміцнення її безпекової системи [11].

Ще одним важливим проєктом, який реалізується в рамках Комплексного пакету допомоги НАТО, є *Спільний центр НАТО-Україна з аналізу, підготовки та освіти (JATEC).* Це перша спільна цивільно-військова інституція НАТО та України, створена для зміцнення взаємосумісності та адаптації української системи безпеки до стандартів Альянсу. Рішення про заснування JATEC було ухвалене на Вашингтонському саміті НАТО у липні 2024 року, а офіційно активований Центр 16 грудня 2024 року. Він розташований у польському місті Бидгощ і підпорядковується Верховному головнокомандувачу Об'єднаних збройних сил НАТО з трансформації [21]. JATEC зосереджений на аналізі військових операцій, інтеграції

уроків війни Росії проти України, розробці стратегічних рішень та впровадженні передових військових практик. Він також сприятиме підготовці військових і цивільних спеціалістів, необхідних для ефективної взаємодії з НАТО. Важливою складовою є створення навчальних програм та обмін досвідом у сфері кризового управління та кооперативної безпеки. Центр є конкретним кроком на шляху України до членства в НАТО. Його діяльність дозволяє не лише впроваджувати євроатлантичні стандарти, а й забезпечує стратегічну інтеграцію України в систему колективної безпеки Альянсу [8].

Політичний контроль і нагляд за реалізацією САР здійснюється *Радою Україна — НАТО (РУН)*, заснованою на Вільнюському саміті НАТО у 2023 році. Цей орган замінив собою Комісію Україна — НАТО та став механізмом, у межах якого Україна бере участь у засіданнях на засадах рівності з державами-членами Альянсу. Головною функцією РУН є забезпечення політичного діалогу, ухвалення рішень і координація спільних заходів у сфері безпеки та оборони. Важливим аспектом діяльності Ради є її роль у проведенні кризових консультацій, які дозволяють оперативно реагувати на виклики, що виникають у сфері кібербезпеки, стратегічних комунікацій та протидії інформаційним загрозам. Особливість РУН полягає в тому, що вона діє не лише як дорадчий орган, а й як структура, яка ухвалює рішення на основі консенсусу між Україною та союзниками. Засідання Ради можуть скликатися на різних рівнях — від глав держав і урядів до міністрів оборони, послів і військових експертів, що забезпечує гнучкість у реагуванні на загрози та ефективну координацію спільних дій [19]. Наприклад, у листопаді 2024 року РУН провела позачергове засідання на рівні послів, присвячене розгляду ситуації після застосування Росією балістичної ракети середнього радіусу дії проти України. Крім того, у межах Ради створено низку підкомітетів, які опікуються питаннями оборонного сектору, стратегічних комунікацій, гібридних загроз і кібербезпеки. Завдяки такій структурі Україна отримує можливість не лише інтегруватися в євроатлантичний безпековий простір, а й активно впливати на ухвалення рішень у сфері інформаційної безпеки та боротьби з дезінформацією [7].

В свою чергу, *Адаптована Річна національна програма (аРНП)* є ключовим стратегічним документом, що визначає пріоритети євроатлантичної інтеграції України та слугує основним механізмом оцінки виконання критеріїв, необхідних для набуття членства в НАТО. Вона є еволюційним продовженням Річних національних програм (РНП), які впроваджувалися з 2009 року як основний інструмент реформ за підтримки Альянсу [23]. Вперше поняття аРНП було введене рішенням Саміту НАТО у Вільнюсі у 2023 році, що підкреслило новий рівень взаємодії України з Альянсом. Програма охоплює п’ять основних напрямів: оборонні та військові питання, політичні та економічні питання, ресурсні питання, питання безпеки та правові питання. У сфері інформаційної безпеки аРНП зосереджена на розвитку кіберзахисту, протидії дезінформації та забезпеченні інформаційної стійкості. Документ передбачає впровадження сучасних технологій захисту інформаційних систем, посилення стійкості критичної

інфраструктури та тісну співпрацю з міжнародними партнерами для обміну досвідом і технологіями. Враховуючи безпекові виклики, пов'язані з російською агресією, аРНП адаптована до умов війни, що дозволяє оперативно реагувати на загрози та інтегрувати зусилля різних відомств задля зміцнення національної безпеки. Координацію виконання програми здійснює *Комісія з питань координації євроатлантичної інтеграції України* під головуванням віце-прем'єр-міністра України, що забезпечує узгодженість заходів та ефективний моніторинг їх реалізації [6].

Зазначимо, що додаткову роль у комунікації та координації співпраці між Україною та НАТО відіграє *Представництво НАТО в Україні*, яке було створене у 2016 році після об'єднання двох структур — Центру інформації та документації НАТО (ЦІДН) та Офісу зв'язку НАТО (NLO). Це рішення стало важливим кроком у поглибленні співробітництва, адже дозволило оптимізувати роботу Альянсу в Україні, спрямовану на підтримку реформ у сфері безпеки та оборони. Основними завданнями Представництва є стратегічна комунікація, надання дорадчої підтримки державним органам, координація допомоги НАТО та сприяння реалізації спільних проєктів. Офіс зв'язку НАТО зосереджений на практичній взаємодії з українськими державними установами, включаючи Міністерство оборони та Раду національної безпеки і оборони, допомагаючи реалізовувати реформи та адаптувати сектор безпеки до стандартів Альянсу. У свою чергу, Центр інформації та документації займається роз'яснювальною роботою, спрямованою на підвищення обізнаності українського суспільства про діяльність НАТО та протидію дезінформації [18]. Останні рішення щодо розширення штату міжнародних представників НАТО в Україні свідчать про наміри посилити безпекову взаємодію та забезпечити ефективну координацію військової допомоги [13]. Одним із ключових елементів цього процесу стало призначення нового спеціального представника НАТО в Україні Патріка Тернера, який приступив до виконання обов'язків у вересні 2024 року [1].

Можемо дійти висновків, що співробітництво між Україною та НАТО у сфері інформаційної безпеки набуває стратегічного значення в умовах сучасних гібридних загроз. Інституційні рамки та механізми взаємодії, включаючи Комплексний пакет допомоги НАТО (CAP), Платформу Україна — НАТО з протидії гібридній війні, участь у CCDCOE та новостворений Центр JATEC, формують багаторівневу систему захисту та зміцнення обороноздатності України. Завдяки цим ініціативам Україна посилює свої спроможності у кібербезпеці, стратегічних комунікаціях, протидії дезінформації та забезпеченні стійкості критичної інфраструктури.

Проте попри прогрес у сфері кібероборони та інформаційної безпеки, високий рівень загроз з боку Росії залишається серйозним випробуванням. Використання дезінформаційних кампаній, втручання у виборчі процеси, масовані кібератаки на критичну інфраструктуру — усе це вимагає не лише потужної технологічної відповіді, але й глибшої координації між урядовими структурами, приватним сектором та міжнародними партнерами.

Перспективи розвитку співпраці з Альянсом залежать від системного підходу до розбудови національної інформаційної безпеки. Зокрема, необхідно посилити спроможності України у сфері контррозвідки, цифрової стійкості та інформаційної протидії, інтегруючи їх у загальну стратегію євроатлантичної інтеграції. Розширення міжнародного партнерства та доступ до передових технологій НАТО, таких, як аналітичні системи на основі ШІ, дасть змогу ефективніше ідентифікувати та нейтралізувати загрози. Останнім найважливішим кроком у цьому напрямі, на нашу думку, стало створення JATEC, який дозволяє систематизувати знання про методи ведення сучасної війни, а також інтегрувати передовий досвід України у військове планування НАТО. Це не лише посилює обороноздатність України, а й робить її важливим безпековим партнером Альянсу.

Отже, поглиблення співпраці з НАТО у сфері інформаційної безпеки є критичним фактором захисту України від гібридних загроз та інтеграції у спільний безпековий простір.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. АрміяInform. Новий спеціальний представник НАТО в Україні: що про нього відомо. 17 липня 2024. URL:https://armyinform.com.ua/2024/07/17/novyj-speczialnyj-predstavnyk-nato-v-ukrayini-shho-pro-nogo-vidomo/
2. Детектор медіа. Нелегітимний Зеленський, могилізація й канонічна церква. Огляд російської дезінформації за 2024 рік. 18 грудня 2024. URL: https://detector.media/monitorynh-internetu/article/236096/2024-12-18-nelegitymnyy-zelenskyy-mogylizatsiya-y-kanonichna-tserkva-oglyad-rosiyskoi-dezinformatsii-za-2024-rik/
3. Детектор медіа. Росія створила в країнах Європи мережу пропагандистських сайтів «Правда» — ЦПД. 8 квітня 2024. URL: https://detector.media/infospace/article/225191/2024-04-08-rosiya-stvoryla-v-krainakh-ievropy-merezhu-propagandystskykh-saytiv-pravda-tspd/
4. Інтерфакс-Україна. НАТО надасть Україні додаткову допомогу у сфері інформаційної безпеки. 5 лютого 2024. URL:https://interfax.com.ua/news/general/951614.html
5. Інтерфакс-Україна. Україна та НАТО посилюють співпрацю у сфері кібербезпеки. 29 лютого 2024. URL: https://interfax.com.ua/news/general/983510.html
6. Міністерство внутрішніх справ України. Реалізація адаптованої річної національної програми на 2024 рік URL: https://mvs.gov.ua/jevroatlanticna-integraciia/realizaciia-adaptovanoyi-ricnoyi-nacionalnoyi-programi-na-2024-rik
7. Міністерство закордонних справ України. Заява Ради Україна — НАТО на рівні міністрів закордонних справ URL: https://mfa.gov.ua/news/zayava-radi-ukrayina-nato-na-rivni-ministriv-zakordonnih-sprav
8. Міністерство оборони України. У Польщі офіційно розпочав роботу Центр НАТО-Україна JATEC URL:https://mod.gov.ua/news/u-polshhi-oficzijno-rozpochav-robotu-czentr-nato-ukraina-jatec
9. Рада національної безпеки і оборони України. Україна стала членом Центру передових технологій з кібероборони НАТО (CCDCOE) URL: https://www.rnbo.gov.ua/ua/Diialnist/6335.html

10. Радіо Свобода. Місія СКУ зафіксувала приклади російської дезінформації про вибори в Україні в іноземних медіа. 22 липня 2019. URL: https://www.radiosvoboda.org/a/30076464.html
11. РБК-Україна. Глава Євроради розповів про прогрес українського питання в НАТО. 23 листопада 2024. URL: https://www.rbc.ua/rus/news/glava-evroradi-rozpoviv-progres-ukrayinskogo-1700764510.html
12. Тиждень. Як працює російська пропаганда в ЗМІ на прикладі RT та Sputnik, 2022 URL: https://tyzhden.ua/iak-pratsiuie-rosijska-propahanda-v-zmi-na-prykladi-rt-ta-sputnik/
13. Укрінформ. Представництво НАТО в Києві може збільшитися вдвічі до кінця року. 10 листопада 2024. URL: https://www.ukrinform.ua/rubric-polytics/3885515-predstavnictvo-nato-v-kievi-moze-zbilsitisa-vdvici-do-kinca-roku.html
14. Центр глобалістики «Стратегія XXI». Співробітництво Україна — ЄС — НАТО з протидії гібридним загрозам у кіберсфері. Київ: Центр глобалістики «Стратегія XXI», 2019.
15. LB.ua. Великий злив: у мережі продають дані мільйонів українців. 23 січня 2022. URL:https://lb.ua/society/2022/01/23/503729_velikiy_zliv_merezhi_prodayut_dani.html
16. Horbulin V. The World Hybrid War: Ukrainian Forefront: monograph abridged and translated from Ukrainian / Volodymyr Horbulin. Харків: Фоліо, 2017. — 158 с.
17. Hurkivska A. Ukraine's Information Security Resilience Amidst Contemporary Warfare: Policy Context in Development. — Kuras Institute of Political and Ethnic Studies, National Academy of Sciences of Ukraine. Södertörn University, 2024.
18. North Atlantic Treaty Organization (NATO). Представництво НАТО в Україні. Офіційний сайт НАТО. URL:https://www.nato.int/cps/uk/natohq/172885.htm
19. North Atlantic Treaty Organization (NATO). Рада Україна — НАТО URL: https://www.nato.int/cps/uk/natohq/topics_231639.htm
20. North Atlantic Treaty Organization (NATO). Comprehensive Assistance Package (CAP) for Ukraine. URL: https://www.nato.int/cps/en/natohq/topics_231639.htm
21. North Atlantic Treaty Organization (NATO). NATO-Ukraine Joint Analysis, Training and Education Centre (JATEC) URL: https://www.act.nato.int/activities/jatec/
22. North Atlantic Treaty Organization (NATO). NATO's approach to countering hybrid threats URL:https://www.nato.int/cps/ru/natohq/topics_156338.htm?selectedLocale=en
23. Shypovskyi V., Cherneha V., Marchenkov S. Analysis of the ways of improvement of Ukraine — NATO cooperation on cybersecurity issues // Social Development & Security. — 2020. — Т. 10, № 2. — С. 11–25. — DOI: 10.33445/sds.2020.10.2.2.
24. The Verge. A deepfake caller pretending to be a Ukrainian official almost tricked a US senator. 26 вересня 2024. URL:https://www.theverge.com/2024/9/26/24255179/deepfake-call-ukraine-senator-cardin-dmytro-kuleba

REFERENCES

1. ArmiiaInform. (2024) Novyi spetsialnyi predstavnyk NATO v Ukraini: shcho pro noho vidomo [The new NATO Special Representative to Ukraine: what we know about him]. Retrived from https://armyinform.com.ua/2024/07/17/novyj-speczialnyj-predstavnyk-nato-v-ukrayini-shho-pro-nogo-vidomo [in Ukrainian].

2. Detektor media. (2024) Nelehitymnyi Zelenskyi, mohylizatsiia y kanonichna tserkva. Ohliad rosiiskoi dezinformatsii za 2024 rik [Illegitimate Zelensky, burial, and the canonical church. An overview of Russian disinformation in 2024]. Retrived from https://detector.media/monitorynh-internetu/article/236096/2024-12-18-nelegitymnyy-zelenskyy-mogylizatsiya-y-kanonichna-tserkva-oglyad-rosiyskoi-dezinformatsii-za-2024-rik/ [in Ukrainian].
3. Detektor media. (2024) Rosiia stvoryla v Ukrainakh Yevropy merezhu propahandystskykh saitiv Pravda [Russia has created a network of Pravda propaganda sites in Europe]. Retrived from https://detector.media/infospace/article/225191/2024-04-08-rosiya-stvoryla-v-krainakh-ievropy-merezhu-propagandystskykh-saytiv-pravda-tspd/ [in Ukrainian].
4. Interfaks-Ukraina. (2024) NATO nadast Ukraini dodatkovu dopomohu u sferi informatsiinoi bezpeky [NATO will provide additional assistance to Ukraine in the field of information security]. Retrived from https://interfax.com.ua/news/general/951614.html [in Ukrainian].
5. Interfaks-Ukraina. (2024) Ukraina ta NATO posyliuiut spivpratsiu u sferi kiberbezpeky [Ukraine and NATO strengthen cooperation in cybersecurity]. Retrived from https://interfax.com.ua/news/general/983510.html [in Ukrainian].
6. Ministerstvo vnutrishnikh sprav Ukrainy. (2024) Realizatsiia adaptovanoi richnoi natsionalnoi prohramy na 2024 rik [Implementation of the adapted annual national program for 2024]. Retrived from https://mvs.gov.ua/jevroatlanticna-integraciia/realizaciia-adaptovanoyi-ricnoyi-nacionalnoyi-programi-na-2024-rik [in Ukrainian].
7. Ministerstvo zakordonnykh sprav Ukrainy. (2023) Zaiava Rady Ukraina — NATO na rivni ministriv zakordonnykh sprav [Statement by the NATO-Ukraine Council at the level of Foreign Ministers]. Retrived from https://mfa.gov.ua/news/zayava-radi-ukrayina-nato-na-rivni-ministriv-zakordonnih-sprav [in Ukrainian].
8. Ministerstvo oborony Ukrainy. (2024) U Polshchi ofitsiino rozpochav robotu tsentr NATO-Ukraina JATEC [NATO-Ukraine JATEC Center officially opens in Poland]. Retrived from https://mod.gov.ua/news/u-polshhi-oficzijno-rozpochav-robotu-czentr-nato-ukraina-jatec [in Ukrainian].
9. Rada natsionalnoi bezpeky i oborony Ukrainy. (2023) Ukraina stala chlenom Tsentru peredovykh tekhnolohii z kiberoborony NATO (CCDCOE) [Ukraine became a member of the NATO Cyber Defense Center of Excellence (CCDCOE)]. Retrived from https://www.rnbo.gov.ua/ua/Diialnist/6335.html [in Ukrainian].
10. Radio Svoboda. (2019) Misiia SKU zafiksuvala pryklady rosiiskoi dezinformatsii pro vybory v Ukraini v inozemnykh media [The UWC Mission documented examples of Russian disinformation about the elections in Ukraine in foreign media. Retrived from https://www.radiosvoboda.org/a/30076464.html [in Ukrainian].
11. RBK-Ukraina. (2024) Hlava Yevrorady rozpoviv pro prohres ukrainskoho pytannia v NATO [President of the European Council tells about the progress of the Ukrainian issue in NATO]. Retrived from https://www.rbc.ua/rus/news/glava-evroradi-rozpoviv-progres-ukrayinskogo-1700764510.html [in Ukrainian].
12. Tyzhden. (2022) Yak pratsiuie rosiiska propahanda v ZMI na prykladi RT ta Sputnik [How Russian propaganda works in the media on the example of RT and Sputnik]. Retrived from https://tyzhden.ua/iak-pratsiuie-rosijska-propahanda-v-zmi-na-prykladi-rt-ta-sputnik/ [in Ukrainian].

13. Ukrinform. (2024) Predstavnytstvo NATO v Kyievi mozhe zbilshytysia vdvichi do kintsia roku [NATO office in Kyiv may double in size by the end of the year]. Retrived from https://www.ukrinform.ua/rubric-polytics/3885515-predstavnictvo-nato-v-kievi-moze-zbilsitisa-vdvici-do-kinca-roku.html [in Ukrainian].
14. Tsentr hlobalistyky Stratehiia 21. (2019) Spivrobitnytstvo Ukraina — YeS — NATO z protydii hibrydnym zahrozam u kibersferi [Ukraine-EU-NATO Cooperation in Countering Hybrid Threats in the Cyberspace]. — Kyiv: Tsentr hlobalistyky Stratehiia 21 [in Ukrainian].
15. LB.ua. (2022) Velykyi zlyv: u merezhi prodaiut dani milioniv ukraintsiv. [The Big Drain: the data of millions of Ukrainians are being sold online]. Retrived from https://lb.ua/society/2022/01/23/503729_velikiy_zliv_merezhi_prodayut_dani.html [in Ukrainian].
16. Horbulin V. (2017) The World Hybrid War: Ukrainian Forefront: monograph abridged and translated from Ukrainian / Volodymyr Horbulin. — Kharkiv: Folio, — 158 p. [in English].
17. Hurkivska A. (2024) Ukraines Information Security Resilience Amidst Contemporary Warfare: Policy Context in Development. — Kuras Institute of Political and Ethnic Studies, National Academy of Sciences of Ukraine. — Södertörn University. [in English].
18. North Atlantic Treaty Organization (NATO). Predstavnytstvo NATO v Ukraini. Ofitsiinyi sait NATO [NATO Representation in Ukraine. Official website of NATO] Retrived from https://www.nato.int/cps/uk/natohq/172885.htm [in English].
19. North Atlantic Treaty Organization (NATO). Rada Ukraina — NATO Retrived from https://www.nato.int/cps/uk/natohq/topics_231639.htm [in English].
20. North Atlantic Treaty Organization (NATO). Comprehensive Assistance Package (CAP) for Ukraine. Retrived from https://www.nato.int/cps/en/natohq/topics_231639.htm [in English].
21. North Atlantic Treaty Organization (NATO). NATO-Ukraine Joint Analysis, Training and Education Centre (JATEC) Retrived from https://www.act.nato.int/activities/jatec/ [in English].
22. North Atlantic Treaty Organization (NATO). NATOs approach to countering hybrid threats Retrived from https://www.nato.int/cps/ru/natohq/topics_156338.htm?selectedLocale=en [in English]
23. Shypovskyi V., Cherneha V., Marchenkov S. (2020) Analysis of the ways of improvement of Ukraine — NATO cooperation on cybersecurity issues // Social Development & Security. T. 10, № 2. — p. 11–25. — DOI: 10.33445/sds.2020.10.2.2. [in English].
24. The Verge. (2024) A deepfake caller pretending to be a Ukrainian official almost tricked a US senator. Retrived from https://www.theverge.com/2024/9/26/2425517 9/deepfake-call-ukraine-senator-cardin-dmytro-kuleba [in English].